Management Software

AT-S45

User's Guide

FOR THE AT-9410GB GIGABIT ETHERNET SWITCH

VERSION 1.0

PN 613-50290-00 Rev A

Allied Telesyn

Simply connecting the IP world

Copyright © 2002 Allied Telesyn, Inc.
960 Stewart Drive Suite B, Sunnyvale, CA 94085 USA

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn, Inc.

Microsoft is a registered trademark of Microsoft Corporation, Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

Table of Contents

Table of Contents 3

List of Figures 8

Preface 10
How This Guide is Organized 10
Document Conventions 11
Where to Find Web-based Guides 12
Contacting Allied Telesyn Technical Support 13
Online Support 13
Telephone Support 13
Management Software Updates 14
For Sales or Corporate Information 15

Section I
Overview 17

Chapter 1

Overview 18
Local Management Session 20
Telnet Management Session 21
Web Browser Management Session 22
SNMP Management Session 23

Section II
Local and Telnet Management 24

Chapter 2

Starting a Local or Telnet Management Session 25
Local Management Session 26
Starting a Local Management Session 27
Quitting from a Local Session 28
Telnet Management Session 29
Starting a Telnet Management Session 29
Quitting from a Telnet Management Session 29

Chapter 3

Basic Switch Parameters 30
When Does an AT-9410GB Switch Need an IP Address? 31
AT-9410GB Switch 31
How Do You Assign an IP Address? 31
Configuring an IP Address 32
Configuring System Administration Information 34
Activating the DHCP Service 36
Configuring SNMP Community Strings and Trap IP Addresses 38
Activating the AT-S45 Management Software Default Values 40
Resetting the Switch 42
Configuring the AT-S45 Management Security Features 43
Viewing the AT-S45 Version Number and Switch MAC Address 46
Pinging a Network Device 47
Bootstrap Configuration 49

Chapter 4

Port Parameters 51
Displaying Port Status 52
Configuring Port Parameters 54

Chapter 5

Port Security 57
Port Security Overview 58
Configuring Port Security 59
Configuring the Limited Security Mode 61

Chapter 6

Port Trunking 63
Port Trunking Overview 64
Creating a Port Trunk 66
Deleting a Port Trunk 69

Chapter 7

Port Monitoring 71
Port Monitoring Overview 72
Creating a Port Monitor 73
Disabling a Port Monitor 75

Chapter 8

Spanning Tree Protocol 76
STP Overview 77
Selecting a Root Bridge 77
Finding and Resolving Redundant Paths 78
Handling Topology Changes 79
Communicating Between Bridges 79
Configuring a Bridge's STP Settings 80
Configuring STP Port Settings 83

Chapter 9

Virtual LANs 86
VLAN Overview 87
VLAN Modes 88
Tagged and Untagged VLAN Overview 89
VLAN Name 89
VLAN Identifier 89

Untagged and Tagged Ports 90
General Rules to Creating an Untagged or Tagged VLAN 92
Creating a Tagged or Untagged VLAN 93
Phase 1 93
Phase 2 96
Viewing or Modifying a Tagged or Untagged VLAN 98
Phase 1 98
Phase 2 100
Deleting a Tagged or Untagged VLAN 103
Port-based VLAN Mode Overview 104
Creating a Port-based VLAN 105
Modifying a Port-based VLAN 107
Setting GVRP Status 109
Resetting the VLAN Parameters to Default 110
Setting the VLAN Type 111

Chapter 10

MAC Address Table 112
MAC Address Overview 113
Displaying MAC Addresses 115
Viewing MAC Addresses by Port 117
Viewing the MAC Addresses by MAC 118
Viewing the MAC Addresses of a VLAN 119
Adding Static MAC Addresses 120
Deleting Static MAC Addresses 121
Changing the Aging Time 122

Chapter 11

Quality of Service 123
Quality of Service Overview 124
Configuring QoS 125

Chapter 12

IGMP Snooping 128
IGMP Snooping Overview 129
Activating IGMP Snooping 130
Viewing Group Members 132

Chapter 13

Storm Control Configuration 135
Storm Control Overview 136
Activating Broadcast Storm Control 137

Chapter 14

Port Statistics 139
Displaying Port Statistics 140

Chapter 15

Management Software Updates 143
Obtaining Software Updates 144
Downloading New Management Software from a Local Management Session 145
Downloading a New Management Software Image Using TFTP 148

Section III
Web Browser Management 152

Chapter 16

Starting a Web Browser Management Session 153
Starting a Web Browser Management Session 154
Browser Tools 155
Quitting from a Web Browser Management Session 156

Chapter 17

Basic Switch Parameters 157
Configuring an IP Address 158
Configuring System Administration Information 160
Setting the User Interface Configuration 162
Activating DHCP 164
Configuring the SNMP Parameters and Trap IP Addresses 166
Resetting a Switch 168
Viewing the AT-S45 Version Number and Switch MAC Address 170
Pinging a Network Device 172
Bootstrap Configuration 174

Chapter 18

Port Parameters 176
Configuring Port Parameters 177
Displaying Port Status 179
Displaying Statistics 182

Chapter 19

Port Security 185
Configuring Port Security 186
Displaying Port Security Settings 188

Chapter 20

Port Trunks 189
Creating or Deleting a Port Trunk 190

Chapter 21

Port Monitoring 192
Creating or Deleting a Port Monitor 193

Chapter 22

Spanning Tree Protocol 195
Configuring a Bridge's STP Settings 196
Configuring STP Port Settings 198

Chapter 23

Virtual LANs 201
Creating a Tagged or Untagged VLAN 202
Phase 1 202
Phase 2 204
Viewing or Modifying a Tagged or Untagged VLAN 206
Phase 1 206
Phase 2 209
Deleting a Tagged or Untagged VLAN 211
Creating a Port-based VLAN 212
Viewing or Modifying a Port-based VLAN 214

Setting GVRP Status 216
Resetting the VLAN Parameters to Default 217
Setting the VLAN Type 218

Chapter 24

MAC Address Table 220
Viewing the MAC Address by Port 221
Viewing the MAC Addresses by MAC 222
Viewing the MAC Addresses of a VLAN 224
Adding Static MAC Addresses 226
Deleting Static MAC Addresses 227

Chapter 25

Quality of Service 228
Configuring QoS 229

Chapter 26

IGMP Snooping 232
Activating IGMP Snooping 233
Viewing Group Members 235

Chapter 27

Storm Control Configuration 236
Activating Broadcast Storm Control and Setting a Threshold 237

Chapter 28

Management Software Updates 239
Obtaining Software Updates 240
Downloading a New Management Software Image Using TFTP 241

Appendix A

AT-S45 Default Settings 245

Index 247

List of Figures

Figure 1: Connecting a Terminal or PC to the RS232 Terminal Port 27
Figure 2: Main Menu 28
Figure 3: Basic Switch Configuration Menu 32
Figure 4: System IP Configuration Menu 33
Figure 5: System Administration Configuration Menu 34
Figure 6: System IP Configuration Menu 37
Figure 7: SNMP Configuration Menu 38
Figure 8: System Reboot Menu 40
Figure 9: User Interface Configuration Menu 44
Figure 10: General Information Window 46
Figure 11: Ping Execution Menu 47
Figure 12: Ping Results 48
Figure 13: Bootstrap Configuration Menu 49
Figure 14: Port Configuration Menu 52
Figure 15: Port Configuration Window 54
Figure 16: Port Security Configuration Menu 59
Figure 17: Intrusion Detection Status Menu 62
Figure 18: Port Trunk Example 1 65
Figure 19: Port Trunk Example 2 65
Figure 20: Trunking Configuration Menu 67
Figure 21: Port Trunk Status Window 68
Figure 22: Port Monitoring Configuration Menu 73
Figure 23: Spanning Tree Configuration Menu 80
Figure 24: Spanning Tree Port Configuration Menu 83
Figure 25: VLAN Management Menu 93
Figure 26: VLAN Creation Menu 94
Figure 27: VLAN Port Configuration Menu 96
Figure 28: Config VLAN Member Menu 99
Figure 29: VLAN Port Configuration Menu 101
Figure 30: VLAN Creation Menu 105
Figure 31: Config VLAN Member Menu 107
Figure 32: Forwarding Database Menu 115
Figure 33: Display MAC Address by MAC Window 116
Figure 34: Quality of Service Configuration Menu 125
Figure 35: IGMP Snooping Configuration Menu 130
Figure 36: View Group Members Menu 132
Figure 37: Broadcast Storm Control Window 137

Figure 38: Ethernet Statistics Menu 140
Figure 39: XModem Software Upgrade Menu 146
Figure 40: Hilgraeve HyperTerminal Window 146
Figure 41: Send File Window 147
Figure 42: XModem File Send Window 147
Figure 43: TFTP Software Upgrade Menu 149
Figure 44: TFTP client software window 150
Figure 45: Entering a Switch's IP Address in the URL Field 154
Figure 46: Home Page 155
Figure 47: IP Configuration menu 158
Figure 48: Administration Configuration menu 160
Figure 49: User Interface 162
Figure 50: IP Configuration 164
Figure 51: SNMP Configuration 166
Figure 52: System Reboot 168
Figure 53: Switch Information 170
Figure 54: Ping Test Configuration 172
Figure 55: Ping Test Result 173
Figure 56: Bootstrap Configuration 174
Figure 57: Port Configuration window 177
Figure 58: Front Panel window 179
Figure 59: Configuration of a Port Window 180
Figure 60: Statistics Window 182
Figure 61: Port Security Window 186
Figure 62: Port Security Overview Window 188
Figure 63: Trunk Configuration Window 190
Figure 64: Port Monitoring Configuration Window 193
Figure 65: Spanning Tree Window - Configuration 196
Figure 66: Spanning Tree Port Configuration 198
Figure 67: Create/Modify VLAN 202
Figure 68: VLAN Port Configuration 205
Figure 69: VLAN Information (802.1Q VLANs) 206
Figure 70: VLAN Create/Modify (802.1Q VLANs) 207
Figure 71: VLAN Port Configuration 209
Figure 72: VLAN Information 211
Figure 73: Confirmation Prompt 211
Figure 74: Create/Modify VLAN 212
Figure 75: VLAN Information (Port-based) 214
Figure 76: Create/Modify VLAN (Port-based VLANs) 214
Figure 77: VLAN Information 216
Figure 78: VLAN Information 217
Figure 79: Sort by Port Window 221
Figure 80: Sort by MAC Window 222
Figure 81: Forwarding Database Configuration - Sort by VLAN Window 225
Figure 82: Static MAC Address Configuration Window 226
Figure 83: Static MAC Address Configuration Window 227
Figure 84: Quality of Service Window 229
Figure 85: IGMP Snooping 233
Figure 86: IGMP Snooping Group Members 235
Figure 87: Broadcast Storm Control Window 237
Figure 88: Image Upgrade Page 241
Figure 89: TFTP client software window 243

Preface

This guide contains instructions on how configure the AT-9410GB Gigabit Ethernet Switch using the AT-S45 management software.

How This Guide is Organized

This manual is divided into three sections.

Section I: Overview

This section has just one chapter. The chapter reviews the different ways that you can access the AT-S45 management software on a switch.

Section II: Local and Telnet Management

The chapters in this section explain how to manage a switch from a local management session or a Telnet management session.

A local management session is established by connecting a terminal or PC to the RS-232 Terminal Port on the front panel of the switch.

A Telnet management session is established using the Telnet application protocol. This type of management session can be performed from any workstation on your network that has the application protocol.

Section III: Web Browser Management

The chapters in this section explain how to manage a switch using a web browser, such as Microsoft® Internet Explorer or Netscape® Navigator.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Where to Find Web-based Guides

The Allied Telesyn web site at www.alliedtelesyn.com contains PDF files of the Installation and User Guides for all Allied Telesyn products. The documents can be viewed on-line or downloaded onto a local workstation or server.

For hardware installation instructions for the AT-9410GB switch, refer to the following guide:

- **AT-9410GB Installation Guide**
  PN 613-50289-00

This guide is available on the documentation CD included with the switch and also from the Allied Telesyn web site.

Contacting Allied Telesyn Technical Support

You can contact Allied Telesyn technical support online or by telephone or e-mail.

Online Support

You can request technical support online by accessing the Knowledge Base from our web site at http://kb.alliedtelesyn.com. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Telephone Support

For Technical Support by telephone, contact Allied Telesyn at one of the following locations:

Americas
United States, Canada, Mexico, Central America, South America
Tel: 1 (800) 428-4835

Asia
Singapore, Taiwan, Thailand, Malaysia, Indonesia, Korea, Philippines, China, India, Hong Kong
Tel: (+65) 3815-612

Australia
Australia, New Zealand
Tel: 1 (800) 000-880

France
France, Belgium, Luxembourg, The Netherlands, Middle East, Africa
Tel: (+33) 1-60-92-15-25

Germany
Germany, Switzerland, Austria, Eastern Europe
Tel: (+49) 30-435-900-126

Italy
Italy, Spain, Portugal, Greece, Turkey, Israel
Tel: (+39) 02-41-30-41

Japan
Tel: (+81) 3-3443-5640

United Kingdom
United Kingdom, Denmark, Norway, Sweden, Finland, Iceland
Tel: (+44) 1-235-442560

Management Software Updates

Allied Telesyn periodically updates the management software programs for our managed products. You can download new versions of our management software from our web site at www.alliedtelesyn.com or our FTP server at ftp.alliedtelesyn.com. To use the FTP server, enter 'anonymous' for the user name when you log in and your e-mail address for the password.

For Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information at the location listed below:

Allied Telesyn, Inc.
19800 North Creek Parkway, Suite 200
Bothell, WA 98011
Tel: 1 (425) 487-8880
Fax: 1 (425) 489-9191

Section I

Overview

The chapter in this section provides a brief overview of the AT-S45 management software. It explains some of the functions that you can perform with the management software and reviews the different methods for accessing the AT-S45 software on an AT-9410GB Gigabit Ethernet Switch.

Chapter 1
Overview

The AT-S45 management software is intended for the AT-9410GB Gigabit Ethernet Switch. You use the software to adjust the operating parameters of the switch. Some of the functions that you can perform with the software include:

- ❑ Enable and disable ports
- ❑ Configure port parameters, such as port speed and duplex mode
- ❑ Create virtual LANs (VLANs)
- ❑ Create port trunks and port mirrors
- ❑ Assign an Internet Protocol (IP) address and subnet mask
- ❑ Activate and configure the Spanning Tree Protocol
- ❑ Configure port security

The AT-S45 management software comes pre-installed on the switch with default settings for all its operating parameters. The default settings may be adequate for some networks and may not need to be changed. If this is true for your network, then you can use the switch as an unmanaged switch by simply connecting the unit to your network, as explained in the hardware installation guide.

Note
The default settings for the management software can be found in **Appendix A, AT-S45 Default Settings** on page 245.

To actively manage a switch, such as to change or adjust its operating parameters, then you must access the switch's AT-S45 management software. The AT-S45 software has a menu interface that makes it very easy to use. It also has a special interface for managing a switch with a web browser.

There are four different ways that you can access the management software on an AT-9410GB Gigabit Ethernet switch. The methods are referred to as management sessions in this guide. They are:

- Local Management Session
- Telnet Management Session
- Web Browser Management Session
- SNMP Management Session

The following sections in this chapter briefly describe each type of management session.

Local Management Session

You establish a local management session with an AT-9410GB Gigabit Ethernet switch by connecting a terminal or a PC with a terminal emulator program to the RS232 Terminal port on the front panel of the switch, using the null-modem management cable include with the switch. This type of management session is referred to as “local” because you must be physically close to the switch, such as in the wiring closet where the switch is located.

Once the session is started, you will see a menu from which you can make selections to configure and monitor the switch. You can configure all of a switch’s operating parameters from a local management session.

Note
For instructions on starting a local management session, refer to **Starting a Local Management Session** on page 27.

Telnet Management Session

Any management workstation on your network that has the Telnet application protocol can be used to manage an AT-9410GB Gigabit Ethernet Switch. This type of management session is referred to in this guide as a remote management session because you can manage the switch from any workstation on your network that has the application protocol.

Establishing a Telnet management session with an AT-9410GB switch requires that the switch have an IP address. You cannot manage an AT-9410GB switch remotely using the Telnet application protocol if it does not have an IP address.

If you are just beginning to build your network and have not assigned any IP addresses to switches, you might want to start by reading **When Does an AT-9410GB Switch Need an IP Address?** on page 31. This section contains a brief discussion about when it makes sense to assign IP addresses to the AT-9410GB switches in your network.

> **Note**
> For instructions on how to start a Telnet management session, refer to **Starting a Telnet Management Session** on page 29.

A Telnet management session gives you complete access to all of a switch's operating parameters. You can perform all the same functions from a Telnet management session as you can from a local management session.

Web Browser Management Session

You can also use a web browser to manage a switch. This too is a type of remote management, just like a Telnet management session, because any workstation on your network that has a web browser can be used to manage a switch.

Note
For instructions on starting a web browser management session, refer to **Starting a Web Browser Management Session** on page 154.

SNMP Management Session

Another way to remotely manage an AT-9410GB switch is with an SNMP management program. A familiarity with Management Information Base (MIB) objects is necessary to manage a switch with an SNMP management program.

The AT-S45 software supports the following MIBs:

- SNMP MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- Interface Group MIB (RFC 1573)
- Ethernet MIB (RFC 1643)
- Remote Network MIB (RFC 1757)
- Allied Telesyn managed switch MIB

You must download the Allied Telesyn managed switch MIB file from the Allied Telesyn web site and compile the file with your SNMP program. For instructions, refer to your SNMP management documentation.

Note
You must assign an IP address to each switch that you want to manage with an SNMP program.

Section II
Local and Telnet Management

The chapters in this section explain how to manage an AT-9410GB Gigabit Ethernet switch from a local or Telnet management session. The chapters include:

- **Chapter 2**: **Starting a Local or Telnet Management Session** on page 25
- **Chapter 3**: **Basic Switch Parameters** on page 30
- **Chapter 4**: **Port Parameters** on page 51
- **Chapter 5**: **Port Security** on page 57
- **Chapter 6**: **Port Trunking** on page 63
- **Chapter 7**: **Port Monitoring** on page 71
- **Chapter 8**: **Spanning Tree Protocol** on page 76
- **Chapter 9**: **Virtual LANs** on page 86
- **Chapter 10**: **MAC Address Table** on page 112
- **Chapter 11**: **Quality of Service** on page 123
- **Chapter 12**: **IGMP Snooping** on page 128
- **Chapter 13**: **Storm Control Configuration** on page 135
- **Chapter 14**: **Port Statistics** on page 139
- **Chapter 15**: **Management Software Updates** on page 143

Chapter 2

Starting a Local or Telnet Management Session

This chapter contains the procedure for starting a local or Telnet management session on an AT-9410GB Gigabit Ethernet Switch. The sections in the chapter are:

- **Local Management Session** on page 26
- **Telnet Management Session** on page 29

Local Management Session

On the front panel of the AT-9410GB switch is a port labelled RS232 Terminal Port. You use this port to establish a local management session with the switch's AT-S45 management software.

A local management session is so named because you must be close to the switch, usually within a few meters, to start this type of management session. This typically means that you must be in the wiring closet where the switch is located.

A switch does not need an IP address for you to manage it with a local management session. You can start a local management session at any time on any AT-9410GB switch in your network. Additionally, running a local management session does not interfere with the flow of Ethernet traffic through the unit.

When you start a local management session on an AT-9410GB switch, you can manage just that switch. To start a local management session on another AT-9410GB switch, you must go to where that switch is located.

Starting a Local Management Session

To start a local management session, perform the following procedure:

1. Connect one end of the management cable included with the switch to the RS232 Terminal Port on the unit.

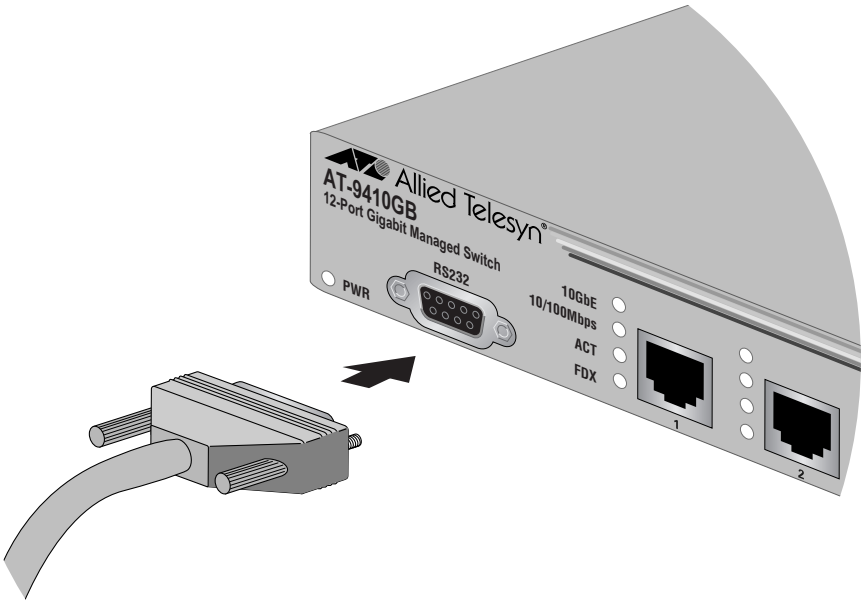

Figure 1 Connecting a Terminal or PC to the RS232 Terminal Port

2. Connect the other end of the cable to an RS-232 port on a terminal or PC with a terminal emulator program.
3. Configure the terminal or terminal emulator program as follows:
   - ❑ Baud rate: 9600
   - ❑ Data bits: 8
   - ❑ Parity: None
   - ❑ Stop bits: 1
   - ❑ Flow control: None

   Note
   The port settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulator program.

4. Press the Return key twice.
5. When prompted for a user name and password, enter the user name and password for the management software. The default for both is "manager". (The user name and password are case-sensitive.)

The Main Menu is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Main Menu

[G]eneral Information
[B]asic Switch Configuration...
[A]dvanced Switch Configuration...
Switch [T]ools...
[S]tatistics
[Q]uit




Command>
```

Figure 2 Main Menu

To select a menu item, type the corresponding letter or number.

Pressing the letter **Q** from a submenu or window returns you to the previous menu.

Quitting from a Local Session

To quit a local session, return to the Main Menu and type **Q** for Quit.

You should always exit from a management session when you are finished managing a switch. This can prevent unauthorized individuals from making changes to a switch's configuration should you leave your management station unattended.

Note
You cannot operate both a local management session and a Telnet management session on the same switch simultaneously. Failure to properly exit from a local or Telnet management session may block future management sessions.

Telnet Management Session

You can use the Telnet application protocol from a workstation on your network to manage an AT-9410GB Gigabit Ethernet Switch. This type of management is referred to as remote management because you do not have to be physically close to the switch to start the session, such as with a local management session. Any workstation on your network that has the application protocol can be used to manage the switch.

In terms of functionally, there are no differences between managing a switch locally through the RS232 Terminal Port and remotely with the Telnet application protocol. You see the same menu selections and have the same management capabilities.

An AT-9410GB switch must have an IP address for you to remotely manage it using the Telnet application protocol. An AT-9410GB switch without an IP address cannot be managed remotely.

Starting a Telnet Management Session

To start a Telnet management session, specify the IP address of the switch in the Telnet application protocol. Enter the management software user name and password when prompted. The default for both is the user name and password "manager" and both are case-sensitive.

The Main Menu of a Telnet management session is the same menu that you see in a local management session, shown in Figure 2 on page 28. All of the functions from a local management session are available to you from a Telnet management session.

The menus also function the same. To make a selection, type the letter enclosed in brackets. To return to a previous menu, type **Q**.

Note
You can run only one Telnet management session on a switch at a time. Additionally, you cannot run both a Telnet management session and a local management session on the same switch at the same time.

Quitting from a Telnet Management Session

To end a Telnet management session, type **Q** for Quit from the Main Menu.

Chapter 3
Basic Switch Parameters

This chapter contains a variety of information and procedures. There is a discussion on when to assign an IP address to a switch and the different ways that you can go about it. There are also procedures for resetting the switch, activating the original switch default settings, and more.

Sections in the chapter include:

- ❑ **When Does an AT-9410GB Switch Need an IP Address?** on page 31
- ❑ **Configuring an IP Address** on page 32
- ❑ **Configuring System Administration Information** on page 34
- ❑ **Activating the DHCP Service** on page 36
- ❑ **Configuring SNMP Community Strings and Trap IP Addresses** on page 38
- ❑ **Activating the AT-S45 Management Software Default Values** on page 40
- ❑ **Resetting the Switch** on page 42
- ❑ **Configuring the AT-S45 Management Security Features** on page 43
- ❑ **Viewing the AT-S45 Version Number and Switch MAC Address** on page 46
- ❑ **Pinging a Network Device** on page 47
- ❑ **Bootstrap Configuration** on page 49

When Does an AT-9410GB Switch Need an IP Address?

One of your first tasks as you begin to build your network will be to determine which of the switches in your network should be assigned unique IP addresses. The following two subsections help to explain how to go about making this decision.

AT-9410GB Switch

Every AT-9410GB switch on your network that you want to manage remotely using the Telnet application protocol, a web browser, or an SNMP management program must have a unique IP address. You cannot remotely manage an AT-9410GB switch if it does not have an IP address. You use the address to identify the switch when you start a remote management session.

If you decide to assign an AT-9410GB switch an IP address, you must also assign it a subnet mask. (The switch uses the subnet mask to determine which portion of an IP address represents the network address and which the node address.)

You must also assign the switch a gateway address if there is a router between the switch and the remote management workstation. This gateway address is the IP address of the router through which the switch and management station will communicate.

You do not need to assign an IP address, subnet mask, or gateway address if you do not intend to manage an AT-9410GB switch remotely. The switch will function fine without these values and you can still configure all switch parameters through a local management session.

How Do You Assign an IP Address?

Once you have decided which, if any, switches on your network need an IP address, you have to access the AT-S45 software on the switches and assign the addresses. You can do this two different ways.

The first method is to assign the IP configuration information manually. The procedure for this is explained in the next procedure. Initially assigning an IP address to a switch can only be done through a local management session.

The second method is by activating the DHCP service on the switch and have the switch automatically download its IP configuration information from a DHCP server on your network. This procedure is explained in **Activating the DHCP Service** on page 36.

Configuring an IP Address

The procedure in this section explains how to manually assign an IP address, subnet mask, and gateway address to the switch from a local or Telnet management session. (If you want the switch to obtain its IP configuration from a DHCP server on your network, go to the procedure **Activating the DHCP Service** on page 36.)

To manually set a switch's IP address, perform the following procedure:

1. From the Main Menu, type **B** to select the Basic Switch Configuration Menu.

   The Basic Switch Configuration Menu in Figure 3 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Main Menu -> Basic Switch Configuration Menu


System [A]dministration Configuration
System [I]P Configuration
S[N]MP Configuration
[P]ort Configuration
[U]ser Interface Configuration
[F]orwarding Database Menu...
[S]panning Tree Configuration
Storm [C]ontrol Configuration
[Q]uit to previous menu




Command>
```

Figure 3 Basic Switch Configuration Menu

2. From the Basic Switch Configuration Menu, type **I** to select System IP Configuration.

The System IP Configuration Menu in Figure 4 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option
Basic Switch Configuration -> System IP Configuration Menu

MAC Address:      00:30:AB:00:09:20
IP Address:       149.35.19.168
Subnet Mask:      255.255.253.0
Default Gateway:  149.35.19.1
DHCP Mode:        Disabled

------------------- <COMMAND> ------------------

Set [I]P Address
Set Subnet [M]ask
Set Default [G]ateway
Enable/Disable [D]HCP Mode
[Q]uit to previous menu



Command>
```

Figure 4 System IP Configuration Menu

3. Change the parameters as desired.

   The commands for changing the parameters are described below:

   Set [I]P Address
   This command specifies the IP address of the switch. You must specify an IP address if you intend to remotely manage the switch using a web browser, a Telnet utility, or an SNMP management program.

   Set Subnet [M]ask
   This command specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch.

   Set Default [G]ateway
   This command specifies the default router's IP address. This address is required if you intend to remotely manage the switch from a management station that is separated from the switch by a router.

Configuring System Administration Information

The procedure in this section explains how to assign a name to the switch, along with other optional information, such as the name of the administrator responsible for maintaining the unit and the location of the switch.

To set the name, contact or location information on a switch, perform the following procedure:

1. From the Main Menu, type **A** to select the System Administration Configuration.

   The System Administration Configuration Menu in Figure 5 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option
Basic Switch Configuration Menu -> System Admin. Configuration Menu

Description:    AT-9410GB
Object ID:      1.3.6.1.4.1.207.1.4.52
Name:
Location:
Contact:

-------------------------- <COMMAND> ----------------------------

Set System [N]ame
Set System [L]ocation
Set System [C]ontact Information
[Q]uit to previous menu



Command>
```

Figure 5 System Administration Configuration Menu

2. Change the parameters as desired. The commands for changing the parameters are described below.

   Set System [N]ame
   This command sets a name for the switch (for example, Sales Ethernet switch). This parameter is optional.

Note
It is advised that you assign each switch a name. The names can help you identify the various switches when you manage them, and can help you avoid performing configuration procedures on the wrong switch.

Set System [L]ocation
This command sets the location of the Gigabit Ethernet switch (for example, 4th Floor - wiring closet 402B). This parameter is optional.

Set System [C]ontact Information
This command sets the name of the network administrator responsible for managing the switch. This parameter is optional.

Activating the DHCP Service

This application protocol was developed to simplify network management. It is used to automatically assign IP configuration information to the devices on your network, such as an IP address, subnet mask, and, in some instances, a default gateway address.

The AT-9410GB Gigabit Ethernet Switch supports this protocol and can obtain its IP configuration information from a DHCP server on your network. If you activate this feature, the switch will seek its IP address and other IP configuration information from a DHCP server. Naturally, for this to work there must be a DHCP server residing on your network and you must configure the service by entering in the switch's MAC address.

Most DHCP services allow you to specify how the IP address is to be assigned to the switch. Choices are static and dynamic. If you choose static, the server will always assign the same IP address to the switch when the switch is reset or powered on. If you choose dynamic, the server will assign any unused IP address that it has not already assigned to another device.

Note
The DHCP option is disabled by default on the switch.

To activate or deactivate the DHCP protocol on the switch, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **I** to select System IP Configuration.

The System IP Configuration Menu in Figure 6 is displayed.

```
AT-9410GB Local Management System

Enter the character in square brackets to select option

Basic Switch Configuration -> System IP Configuration Menu


MAC Address:       00:30:AB:00:09:20
IP Address:        149.35.19.168
Subnet Mask:       255.255.253.0
Default Gateway:   149.35.19.1
DHCP Mode:         Disabled

------------------- <COMMAND> ------------------

Set [I]P Address
Set Subnet [M]ask
Set Default [G]ateway
Enable/Disable [D]HCP Mode
[Q]uit to previous menu



Command>
```

Figure 6 System IP Configuration Menu

3. From the System IP Configuration Menu, type **D** to select Enable/Disable DHCP Mode.

   The following prompt is displayed:

   ```
   Enable or Disable DHCP mode (E/D)>
   ```

4. Enter **E** to enable or **D** to disable the protocol. The default setting is disabled.

   Changes are immediately activated on the switch.

Configuring SNMP Community Strings and Trap IP Addresses

To configure the SNMP community strings for the switch and to assign up to four IP addresses of management stations to receive traps from the switch, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **N** to select SNMP Configuration.

   The SNMP Configuration window in Figure 7 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option
Basic Switch Configuration Menu -> SNMP Configuration Menu

SNMP Read Community: public
SNMP Write Community:private
Trap Authentication: Enable

SNMP Trap Receivers:

No.     Status      IP Address              Community
--      -------    ----------------    ---------------------------
1       Enabled    145.35.19.1             Orion
2       Deleted    <empty>                 <empty>
3       Deleted    <empty>                 <empty>
4       Deleted    <empty>                 <empty>

------------------------- <COMMAND> --------------------------

Set SNMP [R]ead Community                   [A]dd SNMP Trap Receiver
Set SNMP [W]rite Community                  [D]elete SNMP Trap Receiver
[M]odify SNMP Trap Receiver                 [E]nable/Disable
Authentication Trap
Enable/Disable SNMP [T]rap Receiver         [Q]uit to previous menu


Command>
```

Figure 7 SNMP Configuration Menu

3. Adjust the parameters as desired. The commands for changing the parameters are described below.

   Set SNMP [R]ead Community
   This command sets the SNMP community name. The maximum length for a read community name is 20 characters.

   Set SNMP [W]rite Community
   This command sets the SNMP write community. The parameter can be set to private or public.

[M]odify SNMP Trap Receiver
This command specifies trap receiver information. This allows you to modify the IP address and community name of a trap receiver.

Enable/Disable SNMP [T]rap Receiver
This command specifies the status of a trap receiver. This parameter can be set to E for enable or D to disable.

[A]dd SNMP Trap Receiver
This command allows you to add an SNMP trap receiver. The range is set of 1 to 4.

[D]elete SNMP Trap Receiver
This command deletes a specified SNMP trap receiver.

[E]nable/Disable Authentication Trap
This command specifies a community's trap authentication. This parameter can be set to E for enable or D to disable.

Changes to the SNMP parameters are immediately activated on the switch.

Activating the AT-S45 Management Software Default Values

The procedure in this section returns all AT-S45 management parameters to their default values. This procedure also deletes any VLANs that you have created on the switch.

> **Note**
> The AT-S45 default values can be found in **Appendix A**, **AT-S45 Default Settings** on page 245.

To return the AT-S45 management software to its default settings, perform the following procedure:

1. From the Main Menu, type **T** to select Switch Tools.
2. From the Switch Tools Configuration Menu, type **R** to select System Reboot.

   The System Reboot window in Figure 8 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Main Menu -> System Reboot Menu

Reboot Status:        Stop
Reboot Type:          Normal

-------------------------- <COMMAND> ----------------------------

Set Reboot [O]ption
Start [R]eboot Process
[Q]uit to previous menu


Command>
```

Figure 8 System Reboot Menu

3. From the System Reboot Menu, type **O** to select Set Reboot Option.

   The following prompt is displayed:

   ```
   Select reboot option (F/I/N)>
   ```

4. Select the desired reset option. The options are described below.

   F - Factory Defaults
   Resets the switch and returns all parameter settings to their factory default values.

I - Factory Defaults Except IP
Resets the switch and returns all parameter settings, except for the IP address, subnet mask, and gateway address, to their factory default values.

N - Normal Defaults
Resets the switch but retains all current parameter settings.

5. Type **R** to select Reboot.

   The reboot process takes approximately 1 minute to complete.

Resetting the Switch

To reset a switch, perform the following procedure:

1. From the Main Menu, type **T** to select Switch Tools Menu.

> ⚠ **Caution**
> Check the Reboot Type field in the window. It should indicate the reboot type as “Normal”. If this field is indicating Factory Default or Factory Default Except IP, change the setting using the Set Reboot Option command. For further information on the other reboot types, refer to the previous procedure.

2. From the Switch Tools Configuration Menu, type **R** to select System Reboot.
3. From the Switch Tools Menu, type **R** to select Start Reboot Process.

   The following prompt is displayed:

   ```
   Are you sure to reboot the system (Y/N)>
   ```

4. Type **Y** to reset the switch or **N** to cancel the procedure.

   The switch immediately reloads its operating system, a task requiring only seconds to complete.

> ⚠ **Caution**
> The switch will not forward traffic during the brief period required to reload its operating software. Some data traffic may be lost.

Configuring the AT-S45 Management Security Features

The AT-S45 management software has several security features that can help prevent unauthorized individuals from changing the parameter settings of the AT-9410GB switches in your network. These security features are:

- User Name and Password - The management software prompts you for a user name and password whenever you start a local or remote management session on a switch. The default user name and default password are both "manager". The user name and password are case-sensitive. The switches in your network can have the same or different user names and passwords.
- Console and Telnet Timeouts - These parameters cause the management software to automatically end a management session if it does not detect any activity from the local or Telnet management station after the specified period of time. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a switch. The default for the console and Telnet timeout values are 5 (five) minutes.
- Access Methods - You can also disable web browser, Telnet, and SNMP management on the switch, and so prevent individuals from managing the switch remotely using these methods.

To configure the user interface features of the AT-S45 management software, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **U** to select User Interface Configuration.

The User Interface Configuration window in Figure 9 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option
Basic Switch Configuration Menu -> SNMP Configuration Menu

Basic Switch Configuration -> User Interface Configuration Menu

Console UI Idle Timeout:     5 Min.
Telnet UI Idle Timeout:      5 Min.

Telnet Server:       Enabled
SNMP Agent:          Enabled
Web Server:          Enabled
User Name:           manager

---------------------------- <COMMAND> ----------------------------------

Set [C]onsole UI Time Out             Enable/Disable Te[l]net Server
Set [T]elnet UI Time Out              Enable/Disable [S]NMP Agent
Change Administrator User [N]ame      Enable/Disable [W]eb Server
Change Administrator [P]assword       [Q]uit to previous menu


Command>
```

Figure 9 User Interface Configuration Menu

3. Adjust the parameters as desired. The commands for changing the parameters are described below:

   Set [C]onsole UI Time Out
   Configures the console time out in minutes. The switch will automatically end a local management session if it does not detect any management activity after the time period specified with this command.

   For example, if you specify a 2 minute time out, the management software automatically ends the management session if it detects no activity from the terminal connected to the console port after 2 minutes.

   The range is 0 to 60 minutes. A value of “0” means the switch will never time out the management session. The default is 5 minutes.

   Set [T]elnet UI Time Out
   Configures the Telnet time out in minutes. The switch will automatically end a Telnet management session if it does not detect any management activity after the time period specified with this command.

For example, if you specify a 2 minute time out, the management software automatically ends the Telnet management session if it detects no activity from the remote management station after 2 minutes.

The range is 0 to 60 minutes. A value of "0" means the switch will never time out the management session. The default is 5 minutes.

Change Administrator User [N]ame
Sets the login name. The management software will prompt you for this name whenever you start a local or remote management session.

Note
Changing the login name requires entering the current password. You will not be able to change the user name unless you know the password.

Change Administrator [P]assword
Sets the login password. The management software will prompt you for this password whenever you start a local or remote management session.

Note
Changing the login password requires entering the current password.

Enable/Disable Te[l]net Server
Enable/Disable [S]NMP Server
Enable/Disable [W]eb Server
Controls remote management. You can use these three commands to disable remote management of the switch using the Telnet application protocol, an SNMP management program, or a web browser. For example, if you do not want the switch to be managed from a web browser, you would use the Enable/Disable Web Server command to disable this feature on the switch.

Viewing the AT-S45 Version Number and Switch MAC Address

The procedure in this section displays the following switch information:

- ❑ AT-S45 version number
- ❑ Bootloader version number
- ❑ Serial number
- ❑ MAC Address

To display the information, type **G** to select General Information from the Main Menu. The General Information window in Figure 10 is displayed.

```
AT-9410GB Local Management System

Main Menu -> General Information

System up for:   05hr(s), 02min(s), 04sec(s)

Boot Code Version/Date:             1.00A / Dec  8 2001 09:05:22
Runtime Code Version/Date:          1.00E / Jan 15 2002 19:48:12
Hardware Information
  Version:            .            DRAM Size:            8MB
  Fixed Baud Rate:   9600bps        Flash Size:           4MB
Administration Information
  Switch Name: 9410GB
  Switch Location: Lab 304
  Switch Contact: x5260
System Address Information
  MAC Address:       00:30:AB:00:09:20
  IP Address:        149.35.19.249
  Subnet Mask:       255.255.252.0
  Gateway:           149.35.16.1
Automatic Network Features
  DHCP Mode:         Enabled
```

Figure 10 General Information Window

The information in this window cannot be changed.

Pinging a Network Device

This procedure explains how to instruct the switch to ping a network device. This procedure is useful in determining if there is a valid link between the switch and an end node.

To instruct the switch to ping a network device, perform the following procedure:

1. From the Main Menu, type **T** to select Switch Tools.
2. From the Switch Tools Configuration Menu, type **P** to select Ping Execution.

   The Ping Execution Menu is displayed in Figure 11.

```
AT-9410GB Local Management System
Main Menu -> Ping Execution

Target IP Address:     0.0.0.0
Number of Requests:    10
Timeout Value (sec):   3
=============== Result ===============









------------------------------- <COMMAND> -----------------
Set Target [I]P Address                 [E]xecute Ping
Set [N]umber of Requests                [S]top Ping
Set [T]imeout Value                   [Q]uit to previous menu
Command> _
Enter the character in square brackets to select option...
```

Figure 11 Ping Execution Menu

3. Adjust the parameters as desired. To change a value, type its corresponding bracketed letter and, when prompted, enter the new value. The parameters are described below.

   Set Target [I]P Address
   This command specifies the IP address of the end node you want the switch to ping.

   Set [N]umber of Requests
   Number of ping attempts the switch should make before it stops pinging if it does not receive a response. The default number of ping requests is 10.

Set [T]imeout Value
The length of time for which the switch will continue to send pings if it does not receive a response. The default timeout setting is 3 seconds.

4. Select one of the two ping test options by typing the corresponding bracketed letter: Execute Ping or Stop Ping.

   [E]xecute Ping
   Starts the ping process and displays ping test results. Also allows you to clean out the ping test configuration cache by typing **C** for Clean Ping Data. When you clean out the ping data, you will remove the ping test results from view.

   [S]top Ping
   Ends the ping process and displays ping test results gathered before the pinging was stopped.

   An example of the Ping Execution Menu with ping test results is displayed in Figure 12.

```
AT-9410GB Local Management System
Main Menu -> Ping Execution

Target IP Address:     0.0.0.0
Number of Requests:    10
Timeout Value (sec):   3
=============== Result ===============

    No. 1                      60 ms
    No. 2                     100 ms
    No. 3                     100 ms
    No. 4                     100 ms




-------------------------------- <COMMAND> -----------------
Set Target [I]P Address                [E]xecute Ping
Set [N]umber of Requests               [S]top Ping
Set [T]imeout Value                  [Q]uit to previous menu
Command> _
Enter the character in square brackets to select option...
```

Figure 12 Ping Results

The "No." designation indicates the number of the ping attempt. For example, No. 1 represents the first ping attempt.

The milliseconds value represent the time taken for the ping attempt. For example, the first ping test was completed in 60 milliseconds.

Bootstrap Configuration

The bootstrap feature allows you to download new software and configuration settings when you boot up the switch.

To configure the bootstrap settings on the switch, perform the following procedure:

1. From the Main Menu, type **T** to select Switch Tools.
2. From the Switch Tools Configuration Menu, type **B** to select Bootstrap Configuration.

   The Bootstrap Configuration Menu is displayed in Figure 13.

```
AT-9410GB Local Management System
Switch Tools Configuration -> BootStrap Configuration Menu


Boot Load Mode :    Local
Boot Mode :         TFTP
File Type :         IMAGE

----------------------- <COMMAND> ---------------------
Set [B]oot Load Mode
Set Boot [M]ode
Set [F]ile Type
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Figure 13 Bootstrap Configuration Menu

3. Adjust the parameters as desired. To change a value, type its corresponding bracketed letter and, when prompted, enter the new settings. The parameters are described below.

   Set [B]oot Load Mode
   Allows the user to determine how the switch should boot up. There are two boot load options: local and remote.

   - **Local**
     If you choose the local boot load mode, the switch boots using the management software that is saved in the switch memory. This is the default boot load mode. If you are going to use the local boot load mode, you do not need to configure any of the other parameters on the Bootstrap Configuration Menu and the switch will not download any files when it boots up.

- **Remote**
  If you choose the remote boot load mode, the switch downloads software from a TFTP server and boots using the newly downloaded management software.

Set Boot [M]ode
If you are using the remote boot load mode, you need to specify how the switch should download the new management software. There are two boot mode options: DHCP and TFTP.

- **DHCP**
  If you choose the DHCP boot mode, the switch will use DHCP to determine the switch IP address, the TFTP server address, and the image or configuration file name. The switch will use this information to download the management software from the TFTP server.

- **TFTP**
  If you choose the TFTP boot mode, the switch will use the IP address that you assigned to the switch on the System IP Configuration Menu as well as the TFTP server address and the image or configuration file name that you entered in the TFTP section of the Software Upgrade Menu.

Set [F]ile Type
If you selected the remote boot load mode, you can choose what kind of files the switch will download while it is booting up. There are three file type options:

- **Image**
  An image file is the management software for the switch.

- **Configuration**
  A configuration file is a file that contains all of the existing configurations and settings for a switch. You can upload the configuration file and modify the switch settings and then download the configuration file back to the switch or onto multiple switches that you want to have the same configurations. The switch(es) will then update their configuration(s) based on the settings in the configuration file.

- **Image and Configuration**
  This option allows you to download both the management software and the configuration file.

Chapter 4

Port Parameters

The chapter contains procedures for viewing and changing the parameter settings for the individual ports on a switch.

This chapter contains the following procedures:

- ❑ **Displaying Port Status** on page 52
- ❑ **Configuring Port Parameters** on page 54

Displaying Port Status

To display the status of the ports on the switch, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **P** to select Port Configuration.

   The Port Configuration Menu in Figure 14 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option
Basic Switch Configuration -> Port Configuration Menu

Port   Trunk   Type     Link     Status       Mode        Flow Ctrl
----   -----   ------   -----    ----------   -------     ---------
1       ---    1000TX   Down     Enabled      Auto        Enabled
2       ---    1000TX   Down     Enabled      Auto        Enabled
3       ---    1000TX   Down     Enabled      Auto        Enabled
4       ---    1000TX   Down     Enabled      Auto        Enabled
5       ---    1000TX   Down     Enabled      Auto        Enabled
6       ---    1000TX   Down     Enabled      Auto        Enabled
7       ---    1000TX   Down     Enabled      Auto        Enabled
8       ---    1000TX   Down     Enabled      Auto        Enabled
9       ---    1000TX   Down     Enabled      Auto        Enabled
10      ---    1000TX   Down     Enabled      Auto        Enabled
11      ---    1000X    Down     Enabled       1000-FDx   Enabled
12      ---    1000X    Down     Enabled       1000-FDx   Enabled
-------------------------- <COMMAND> ----------------------------

Set [S]tatus                              Set [F]low control
Set [M]ode                                [Q]uit to previous menu


Command>
```

Figure 14 Port Configuration Menu

The columns in the window are described below:

Port
The port number.

Trunk
The trunk group number. A number in this column indicates that the port is a member of a port trunk.

Type
The maximum operating speed of the port.

Link
The link status between the port and the end node connected to the port. Possible values are:

Up - indicates that a valid link exists between the port and the end node.

Down - indicates that the port and the end node have not established a valid link.

Status
The current operating status on the port. Possible values are:

Enabled - Indicates that the port is enabled.

Disabled - Indicates that the port is disabled.

Mode
The operating mode of the port. Possible values are:

- Auto-Negotiate: The port will Auto-Negotiate both speed and duplex mode. This is the default.
- 1000Mbps - Half Duplex
- 100Mbps - Full Duplex
- 10Mbps - Full Duplex
- 1000Mbps - Half Duplex
- 100Mbps - Half Duplex
- 10Mbps - Half Duplex

Flow Control
The flow control setting for the port. Possible values are:

Disabled - No flow control on the port.

Enabled - Flow control is activate on the port.

Configuring Port Parameters

To configure the parameter settings for a port on the switch, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **P** to select Port Configuration.

   The Port Configuration Menu in Figure 15 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option
Basic Switch Configuration -> Port Configuration Menu

Port   Trunk  Type    Link     Status       Mode       Flow Ctrl
----   -----   ------   -----   ----------   -------   ---------
1      1      1000TX  Down     Enabled       1000-FDx  Disabled
2      1      1000TX  Down     Enabled       1000-FDx  Disabled
3      1      1000TX  Down     Enabled       1000-FDx  Disabled
4      1      1000TX  Down     Enabled       1000-FDx  Disabled
5      ---    1000TX  Down     Enabled      Auto       Enabled
6      ---    1000TX  Down     Enabled      Auto       Enabled
7      ---    1000TX  Down     Enabled      Auto       Enabled
8      ---    1000TX  Down     Enabled      Auto       Enabled
9      ---    1000TX  Down     Enabled      Auto       Enabled
10     ---    1000TX  Down     Enabled      Auto       Enabled
11     ---    1000X   Down     Enabled       1000-FDx  Enabled
12     ---    1000X   Down     Enabled       1000-FDx  Enabled
-------------------------- <COMMAND> ----------------------------

Set [S]tatus                          Set [F]low control
Set [M]ode                            [Q]uit to previous menu


Command>
```

Figure 15 Port Configuration Window

3. Set the port parameters as desired. To set a parameter, type the letter of the appropriate command. This toggles the parameter through its possible settings. The commands are described below.

   Set [S]tatus
   You use this command to enable or disable a port. When disabled, a port will not receive or transmit frames.

You might want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the port again to resume normal operation. You can also disable an unused port to secure it from unauthorized connections.

Possible settings are:

Enabled - The port will receive and forward packets. This is the default setting.

Disabled - The port will not receive or forward packets.

Set [M]ode
You use this selection to manually configure a port's speed and duplex mode.

Auto-Negotiation is the default setting. In the Auto-Negotiation setting, the switch will set both speed and duplex mode for the port automatically.

The additional selections are displayed in the command prompt:

```
Enter new mode for port 1 (a/h/H/f/F/t/T)>
```

The possible settings for this selection are:

- a - Auto (Auto-Negotiation)
- h - 10-HDx (10 Mbps, half-duplex)
- H - 100-HDx (100 Mbps, half-duplex)
- f - 10-FDx (10 Mbps, full-duplex)
- F - 100-FDx (100 Mbps, full-duplex)
- t - 1000-HDx (1000 Mbps, half-duplex)
- T - 1000-FDx (1000 Mbps, full-duplex)

Note
Ports 11 and 12 are automatically set to the default setting of 1000-FDx.

Set [F]low Control
Flow control applies only to ports operating in full-duplex mode. The switch uses a special pause packet to stop the end node from sending frames. The pause packet notifies the end node to stop transmitting for a specified period of time.

Possible settings are:

Disabled - No flow control on the port.

Enabled - Flow control for both packets entering and leaving the port.

Configuration changes are immediately activated on a port.

Chapter 5
Port Security

This chapter contains the procedures for setting port security. The sections in this chapter include:

- ❑ **Port Security Overview** on page 58
- ❑ **Configuring Port Security** on page 59
- ❑ **Configuring the Limited Security Mode** on page 61

Note
Port security does not apply to ports on GBIC modules in an AT-9410GB switch.

Port Security Overview

The port security feature can enhance the security of your network. You can use the feature to control the number of MAC addresses learned on the ports, and so control the number of network devices that can forward frames through the switch.

There are four levels of port security. The security level can be set on a per port basis.

Normal
This operating mode disables port security. The switch learns and adds addresses to its dynamic MAC address table as it receives frames on the ports.

> **Note**
> The Normal security mode is the default security level for the switch.

Limited
You can use this security level to specify the maximum number of dynamic MAC addresses a port on the switch can learn. Once a port has learned its maximum limit of MAC addresses, it discards ingress frames with source MAC addresses not already stored in the MAC address table.

The MAC aging time remains active under this security level. Inactive dynamic MAC addresses learned on a port are aged out of the table.

> **Note**
> Static MAC addresses are retained by the switch and are not included in the count of maximum addresses that can be learned by a port. You can continue to add static MAC addresses to a port even if the port has already learned its maximum number of dynamic MAC addresses.

Secure
The Secure level stops a port from learning any new dynamic MAC addresses. The port will forward ingress frames based on the dynamic MAC addresses it has already learned and on any static MAC addresses.

The dynamic MAC addresses learned are not aged out of the table, even when an end node is inactive.

You can continue to add static MAC addresses to a port operating under this security level.

Configuring Port Security

To set a switch's port security level, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.
2. From the Advanced Switch Configuration Menu, type **P** to select Port Security Configuration.

   The Port Security Configuration Menu in Figure 16 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option
Advanced Switch Configuration -> Port Security Configuration Menu

Port    Secure Level     Threshold     Intrusion Detection Status
----   --------------   ------------   --------------------------
1       Secure           -----          No action
2       Secure           -----          No action
3       Secure           -----          Notify with trap only
4       Secure           -----          No action
5       Secure           -----          No action
6       Secure           -----          No action
7       Secure           -----          No action
8       Secure           -----          No action
9       Secure           -----          No action
10      Secure          -----           No action
11      Secure          -----           No action
12      Secure          -----           No action
------------------------- <COMMAND> ----------------------------
[S]et Secure Level                     Set [T]hreshold
Set Intrusion [D]etection              [Q]uit to previous menu


Command>
```

Figure 16 Port Security Configuration Menu

3. To select the desired security level, type **S** to select Set Secure Level.

   The following prompt is displayed:

   ```
   Set secure level->Enter port number >
   ```

4. Enter the number of the port you want to configure. Press Return.

   The following prompt is displayed:

   ```
   Limited or Secure port (L/S/N)>
   ```

5. Select the desired security level:

   - ❑ To disable security on a port, type **N** to select Normal mode. This is the default setting.
   - ❑ To specify a maximum number of MAC addresses the port can learn, type **L** to select Limited mode. To specify the limit, perform the procedure in **Configuring the Limited Security Mode** on page 61.
   - ❑ To stop a port from learning new dynamic MAC addresses, type **S** to select the Secured mode.

   A change to the security level is immediately activated on the port.

Configuring the Limited Security Mode

The Limited security mode lets you set a maximum number of dynamic MAC addresses a port on a switch can learn. Once the maximum number of MAC addresses have been learned by a port, frames with new source MAC addresses are discarded and are not forwarded by the port.

Static MAC addresses are not included in the count of the maximum MAC addresses a port can learn. You can continue to add static MAC addresses even after a port has learned its maximum number of dynamic MAC addresses.

To configure Limited security mode for a port, perform the following procedure:

1. Perform the procedure **Configuring Port Security** on page 59 to configure the port with Limited security.
2. Type **T** to select Set Threshold.

   The following prompt is displayed:

   ```
   Set threshold->Enter port number >
   ```
3. Enter the number of the port you want to configure. Press Return.

   The following prompt is displayed:

   ```
   Set threshold->Enter port number >
   ```
4. Enter a Threshold value. The range is 1 thru 170 MAC addresses. Press Return.

   Note
   Threshold is not supported in Normal and Secure modes.

5. Type **D** to select Set Intrusion Detection.

   The following prompt is displayed:

   ```
   Set intrusion detection status->Enter port number >
   Port number is in range of 1 to 12
   ```
6. Enter the number of the port to configure. Press Return.

The Intrusion Detection Status menu in Figure 17 is displayed

```
AT-9410GB Local Management System
Select item number for intrusion detection status

Advanced Switch Configuration -> Port Security Configuration Menu

Item                Description
------  ------------------------------------
1               No action
2               Disable the port only
3               Notify with trap only
4               Notify with trap and disable the port




Set intrusion detection status->Enter item number >
```

Figure 17 Intrusion Detection Status Menu

7. Type the number associated with the desired setting for Intrusion Detection Status. The following parameters are available:

   1 - No action
   2 - Disable the port only
   3 - Notify with trap only
   4 - Notify with trap and disable the port

Note
Intrusion Detection is not supported in Normal and Secure modes.

Chapter 6
Port Trunking

This chapter contains the procedures for creating and deleting port trunks. Sections in the chapter include:

- ❑ **Port Trunking Overview** on page 64
- ❑ **Creating a Port Trunk** on page 66
- ❑ **Deleting a Port Trunk** on page 69

Port Trunking Overview

Port trunking is an economical way for you to increase the bandwidth between an AT-9410GB Gigabit Ethernet Switch and another network device, such as a server, router, workstation, or another switch. A port trunk is two or more data ports that have been grouped together to increase the bandwidth between a switch and a network node by functioning as one logical path. This increase in bandwidth can prove useful in situations where a single connection between the switch and a node is insufficient to handle the traffic load.

Port trunks are also useful in adding redundancy to the critical devices of your network. If one link of a port trunk fails, the remaining links will continue to provide a communications link to the end node.

Despite the software configuration and physical connections, there are no data loops in a port trunk because of load balancing. The port trunk always sends packets from a particular source to a particular destination over the same link within the trunk. A single link is designated for flooding broadcasts and packets of unknown destination.

Below are the guidelines to follow when planning a port trunk:

- ❑ The switch can support up to four port trunks at a time.
- ❑ A port trunk can have as many as four ports.
- ❑ A port can be a member of only one trunk at a time.
- ❑ The duplex mode, speed, and flow control settings must be the same for all of the ports in a trunk.
- ❑ The ports of a port trunk must be members of the same VLAN. A port trunk cannot consist of ports that are members of different VLANs.
- ❑ When cabling a trunk, the order of the connections should be maintained on both nodes. The lowest numbered port in a trunk on the switch should be connected to the lowest numbered port of the trunk on the other device, the next lowest numbered port on the switch should be connected to the next lowest numbered port on the other device, and so on.

  For example, assume that you are connecting a trunk between two AT-9410GB switches. On the first AT-9410GB switch you had chosen ports 2, 3, 4, and 5 for the trunk. On the second AT-9410GB switch you had chosen ports 1, 2, 3, and 4. To

maintain the order of the port connections, you would connect port 2 on the first AT-9410GB switch to port 1 on the second AT-9410GB, port 3 to port 2, and so on.

- ❑ The ports of a port trunk must be of the same type. For example, they can be all twisted pair ports or all fiber optic ports.
- ❑ You can create a port trunk of the GBIC modules installed in the GBIC1 and GBIC2 slots, provided that the GBIC modules are of the same type.
- ❑ The ports on the end node must also be configured as a port trunk.

Figure 18 shows an example of a port trunk between an AT-9410GB switch and a network server. The server is connected to the switch with four data links. The links are connected to ports 1 through 4 on the switch.

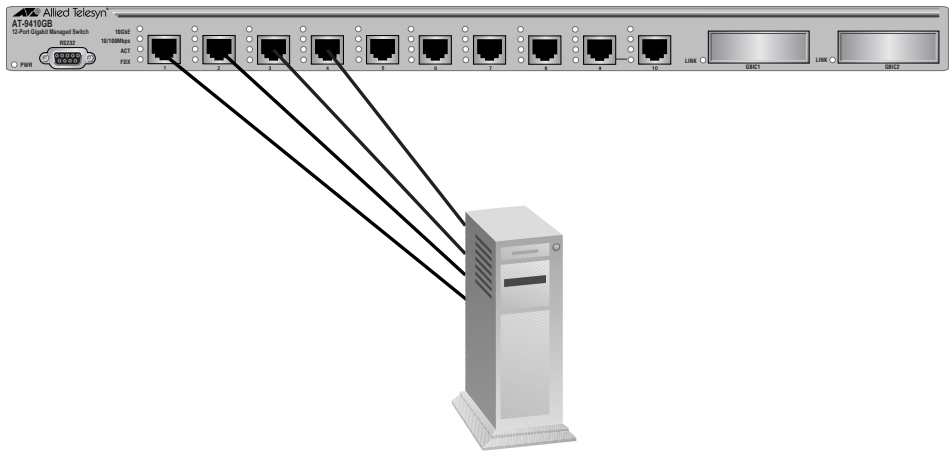

Figure 18 Port Trunk Example 1

You can also use port trunks to increase the bandwidth between switches. The example in Figure 19 shows a port trunk of four data links between two AT-9410GB Gigabit Ethernet switches.

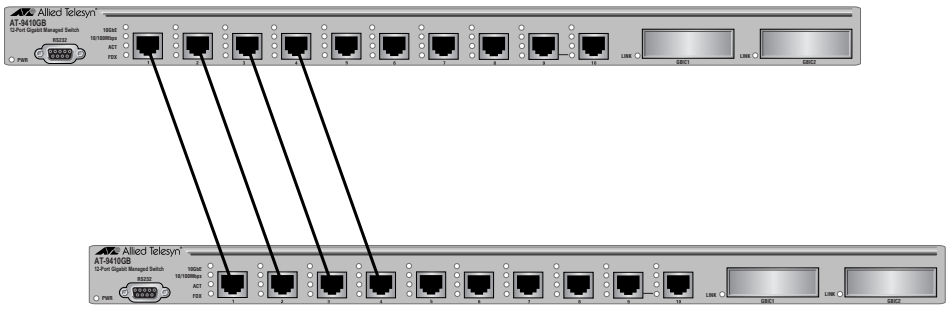

Figure 19 Port Trunk Example 2

Creating a Port Trunk

This section contains the procedure for creating a port trunk on the switch. Be sure to review the guidelines in **Port Trunking Overview** on page 64 before performing the procedure.

Caution
Do not connect the cables to the trunk ports on the switch until after you have configured the trunk with the management software. Connecting the cables before configuring the software will create a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

Note
Before creating a port trunk, examine the parameter settings of the ports that will make up the trunk. Check to be sure that the settings, such as speed and duplex mode, are the same for all the ports of the trunk. You should also check to be sure that the ports are members of the same VLAN.

To create a port trunk, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.
2. From the Advanced Switch Configuration Menu, type **T** to select Trunk Configuration.

   The Trunking Configuration Menu in Figure 20 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Advanced Switch Configuration -> Trunk Configuration Menu

Group   Status   Port Members
-----  --------  --------------------------------
1      Disabled
2      Disabled
3      Disabled
4      Disabled

Note: The trunk port members must be within the same port group.
The port members of each port group are shown below.

----------------------- <COMMAND> ------------------------

[A]dd Trunk Member                    [S]et Trunk status
[R]emove Trunk Member                 [Q]uit to previous menu

Command>
```

Figure 20 Trunking Configuration Menu

3. Type **A** to select Add Trunk Member.

   The following prompt is displayed.

   ```
   Enter trunk group number>
   Trunk group is in the range from 1 to 4
   ```

4. Enter the trunk group number to configure and press Return.

   The following prompt is displayed.

   ```
   Enter port members (up to 4 ports) for trunk 1>
   Separate each port number with a comma;
   Specify a range of ports by a hyphen
   ```

5. Enter the ports that will constitute the port trunk and press Return.

   You can specify up to a maximum of 4 ports either individually (e.g., 1,2,3,4) or as a range (e.g., 7-10).

6. To set trunk status, type **S** to display the status of the trunk.

   The following prompt is displayed.

   ```
   Enter trunk group number>
   Trunk group is in the range from 1 to 4
   ```

7. Enter the trunk group number you want to set and press Return.

   The following prompt is displayed.

   ```
   Enable or Disable trunk group 1 (E/D)>
   E for Enable; D for Disable
   ```

8. Type **E** to enable the new port trunk.

   Figure 21 shows an example of the Port Trunking status window with a port trunk.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Advanced Switch Configuration -> Trunk Configuration Menu

Group   Status   Port Members
-----  --------  -------------------------------
1      Enabled    1,  2,  3,  4
2      Disabled
3      Disabled
4      Disabled

Note: The trunk port members must be within the same port group.
The port members of each port group are shown below.

---------------------- <COMMAND> -----------------------

[A]dd Trunk Member                    [S]et Trunk status
[R]emove Trunk Member                 [Q]uit to previous menu

Command>
```

Figure 21 Port Trunk Status Window

9. Configure the ports on the remote end node for port trunking. Refer to the instructions included with the node for directions on how to create a port trunk.
10. Connect the cables to the ports of the trunk on the switch.

    The port trunk is ready for network operations.

Deleting a Port Trunk

Caution
Disconnect the cables from the port trunk on the switch before performing the following procedure. Deleting a port trunk without first disconnecting the cables can create loops in your network topology. Data loops can result in broadcast storms and poor network performance.

To delete a port trunk from the switch, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.
2. From the Advanced Switch Configuration Menu, type **T** to select Trunk Configuration.

   The Port Trunking menu in Figure 20 on page 67 is displayed.
3. Type **R** to select Remove Trunk Member.

   The following prompt is displayed.

   ```
   Enter trunk group number>
   Trunk group is in the range from 1 to 4
   ```
4. Enter the trunk group number you want to remove and press Return.

   The following prompt is displayed.

   ```
   Enter port members (up to 4 ports) for trunk 1>
   Separate each port number with a comma;
   Specify a range of ports by a hyphen
   ```
5. Enter the port members of the trunk and press Return.

Note
You must delete all port members from a trunk group in order to delete a trunk. Disabling a trunk group will not delete the port members from a trunk group and could cause a data loop.

The Trunk Configuration window should now show that the port trunk has been removed from the switch.

Chapter 7
Port Monitoring

This chapter contains the procedures for creating and deleting a port monitor. Sections in the chapter include:

- ❑ **Port Monitoring Overview** on page 72
- ❑ **Creating a Port Monitor** on page 73
- ❑ **Disabling a Port Monitor** on page 75

Port Monitoring Overview

The port monitoring feature allows you to unobtrusively monitor the traffic being received and transmitted on a port on a switch by having the traffic copied to another switch port. You can connect a network analyzer to the port where the traffic is being copied and monitor the traffic on the other port without impacting network performance or speed.

Observe the following guidelines when creating a port trunk:

- ❑ You can monitor only one port on a switch at a time.
- ❑ The port to be monitored and the monitoring port must be located on the same switch.
- ❑ The port to be monitored and the monitoring port must be operating at the same speed. For example, you cannot use a 10/100 Mbps port to monitor traffic on a 1000 Mbps GBIC port.

Creating a Port Monitor

To create a port monitor, perform the following procedure:

1. From the Main Menu, type **A** to select Switch Advanced Configuration.
2. From the Switch Advanced Configuration Menu, type **M** to select Port Monitoring Configuration Menu.

   The Port Monitoring Configuration Menu in Figure 22 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Advanced Switch Configuration -> Port Monitoring Configuration Menu

Monitoring Port   Monitored Port      Status
---------------   --------------    -----------
1                  4                 Enabled


------------------------- <COMMAND> -----------------------------

[S]et Monitoring Port
Set [M]onitored Port
[E]nable/Disable Port Monitoring
[Q]uit to previous menu



Command>
```

Figure 22 Port Monitoring Configuration Menu

3. Type **S** to select Set Monitoring Port.

   The following prompt is displayed.

   ```
   Set monitoring port->Enter port number>
   Port number is in range of 1 to 12
   ```

4. Enter the number of the port to function as the monitor port (that is, the port to where the traffic will be copied). Press Return.

   You can specify only one monitor port.

5. Type **M** to select Set Monitored Port.

   The following prompt is displayed.

   ```
   Set monitored port->Enter port number>
   Port number is in range of 1 to 12
   ```

6. Enter the number of the port whose traffic is to be monitored. You can specify only one port to be monitored.

7. Type **E** to select Enable/Disable Port Monitoring.

   The following prompt is displayed.

   ```
   Enable or Disable monitoring (E/D)>
   E for Enable; D for Disable
   ```

8. Type **E** to activate the port monitor.
9. To confirm the creation of the port monitor, view the Status area in the Port Monitoring Configuration menu displayed in Figure 22.

   The management software displays the number of the monitor port and the port whose traffic is to be monitored.

   The port monitor is now functional.

Disabling a Port Monitor

To disable a port monitor, perform the following procedure:

1. From the Main Menu, type **A** to select Switch Advanced Configuration Menu.
2. From the Switch Advanced Configuration Menu, type **M** to select Port Monitoring Configuration Menu.

   The Port Monitoring Configuration menu in Figure 22 on page 73 is displayed.
3. Type **E** to select Enable/Disable Port Monitoring.

   The following prompt is displayed.

   ```
   Enable or Disable monitoring (E/D)>
   ```
4. Enter **D** to disable port monitoring.

   The port monitor on the switch is now disabled. The port that was functioning as the port monitor is now available for normal network operations.

Chapter 8
Spanning Tree Protocol

This chapter provides introductory information on the Spanning Tree Protocol (STP) and explains how to adjust the STP bridge and port parameters. The sections in this chapter include:

- ❑ **STP Overview** on page 77
- ❑ **Configuring a Bridge's STP Settings** on page 80
- ❑ **Configuring STP Port Settings** on page 83

Note
For detailed information on the Spanning Tree Protocol, refer to Section 4 of IEEE Std 802.1D, ISO/IEC 10038: 1993.

STP Overview

The AT-9410GB Gigabit Ethernet Switch supports the Spanning Tree Protocol, as specified in the IEEE 802.1D standard. STP can be an important part of large networks where loops, either planned or unplanned, exist in the network topology.

A loop exists when two or more nodes on your network can transmit data to each other over more than one data link. A network loop can pose a danger to network performance and operability. Data packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and often significantly reduce network performance.

STP prevents data loops from forming in your network by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, STP places the extra paths in a standby or blocking mode, leaving only one main active path.

The redundant paths can be activated by STP if the main path goes down. So not only does STP guard against multiple links between end nodes, but it can also activate backup redundant paths in case a main link fails.

Selecting a Root Bridge

The first task that bridges perform when STP is activated on a network is the selection of a *root bridge*. The root bridge is used by the other bridges to determine if there are redundant paths in the network. The root bridge also distributes network topology information to the other network bridges.

A root bridge is selected by a combination of a bridge's priority number, also referred to as the bridge identifier, and sometimes its MAC address. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same bridge priority number, of those bridges the one with the lowest MAC address is designated as the root bridge.

The bridge priority number is adjustable on the AT-9410GB Switch. By adjusting the value, you can designate which switch on your network you want as the root bridge by giving it the lowest bridge priority number. You should probably also consider which bridge should function as a backup in the event you need to take the primary root bridge off-line, and assign that bridge the second lowest bridge identifier number.

Finding and Resolving Redundant Paths

Once the Root Bridge has been selected, the bridges must determine if the network contains redundant paths and, if one is found, they must select a preferred path while placing the redundant paths in a backup or blocking state.

Where there is only one path between a bridge and a root bridge, the bridge is referred to as the *designated bridge* and the port through which the bridge is communicating with the root bridge is referred to as the *designated port*.

If redundant paths exist, the bridges that are a part of the paths must determine which path will be the primary, active path, and which path(s) will be placed in the standby, blocking mode. This is accomplished by an evaluation of port costs. The path offering the lowest cost to the root bridge becomes the primary path and all other redundant paths are placed into blocking state.

Every port on a bridge participating in STP has a cost associated with it. The cost of a port on a bridge is typically based on port speed. The faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

Below are standard default values for port costs. The port costs of the ports on the AT-9410GB Gigabit Ethernet Switch are adjustable through the management software.

Table 1 Standard Port Costs

Port Speed	Port Cost
10 Mbps	100
100 Mbps	10
1000 Mbps	4

The cost of a path is cumulative; the final cost of a path is the value of all ports between a bridge and the root bridge.

The AT-S45 management software assumes that the ports will operate at 1000 Mbps. It assigns each port a default path cost of 4. If a port will be operating at a slower speed, you may want to change its port cost.

If two paths have the same port cost, the preferred path is selected through *port priority*. This too is a value that you can adjust on a per port basis on the switch.

Handling Topology Changes

If there is a change in the network topology due to a failure, removal, or addition of any active components, the active topology also changes. This may trigger a change in the state of some blocked ports. However, a change in a port state is not activated immediately.

It might take time for the root bridge to notify all bridges that a topology change has occurred, especially if it is a large network. If a topology change is made before all bridges have been notified, a temporary data loop could occur, and that could adversely impact network performance.

To forestall the formation of temporarily data loops during topology changes, a port designated to change from blocking to forwarding passes through two additional states, listening and learning, before it begins to forward frames. The amount of time a port spends in these states is set by the *Forwarding Delay* value. This value states the amount of time that a port spends in the listening and learning states prior to changing to the forwarding state.

The Forwarding Delay value is adjustable on the AT-9410GB Gigabit Ethernet Switches through the management software. The appropriate value for this parameter will depend on a number of variables, with the size of your network being a primary factor. For large networks, you should specify a value large enough to allow the root bridge sufficient time to propagate a topology change throughout the entire network. For small networks, you should not specify a value so large that a topology change is unnecessarily delayed, which could result in the delay or loss of some data packets.

Communicating Between Bridges

The bridges that are part of a spanning tree domain communicate with each other using a bridge broadcast frame that contains a special section devoted to carrying STP information. This portion of the frame is referred to as the Bridge Packet Data Unit (BPDU). When a bridge is brought on-line, it will issue a BPDU in order to determine whether a root bridge has already been selected on the network. and if not, whether it has the lowest bridge priority number of all the bridges and should therefore become the root bridge.

The root bridge will periodically transmit a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the *Hello Time*. This is a value that you can set on the AT-9410GB Gigabit Ethernet Switches. The interval is measured in seconds and the default is 2 seconds. Consequently, if an AT-9410GB Switch is selected as the Root Bridge of a spanning tree domain, it will transmit a BPDU every two seconds.

Configuring a Bridge's STP Settings

This section contains the procedure for configuring a bridge's STP settings.

Caution
STP on a bridge is disabled by default. If you enable STP, the bridge provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **S** to select Spanning Tree Configuration Menu.

   The Spanning Tree Configuration Menu is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Basic Switch Configuration -> Spanning Tree Configuration Menu

STP Status:      Enabled

Root Port:       0
Root Path Cost:  0

Designated Root: 8000 0030AB000850   Bridge ID: 8000 0030AB000920
Hello Time:      2     Sec.          Bridge Hello Time:    2     Sec.
Maximum Age:     20    Sec.          Bridge Maximum Age:   20    Sec.
Forward Delay:   15    Sec.          Bridge Forward Delay: 15    Sec.

---------------------------- <COMMAND> ------------------------------

Enable/Disable [S]TP             Set Bridge Maximum [A]ge
Set Bridge Pr[i]ority            Set Bridge Forward [D]elay
Set Bridge [H]ello Time          Spanning Tree [P]ort Configuration
[Q]uit to previous menu



Command>
```

Figure 23 Spanning Tree Configuration Menu

The window displays the current STP operating parameters in two columns labeled Designated Root and Bridge ID. The column labeled Designated Root displays the STP parameters from the root bridge. The parameters in the Bridge ID column are from the AT-9410GB switch you are currently managing.

3. Adjust the bridge STP settings as needed. The commands for setting the parameters are described below.

   Enable/Disable [S]TP
   Enables and disables STP on the switch. The default setting is disabled.

   Set Bridge Pr[i]ority
   Sets the priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 65,535, with 0 being the highest priority.

   The default value for bridge priority for an AT-9410GB switch is 8000. The current value for the unit is displayed in the Bridge ID field in the window and is followed by the MAC address (i.e., Bridge ID: 8000 0030AB000920).

   Set Bridge [H]ello Time
   Sets the time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

   Set Bridge Maximum [A]ge
   Sets the length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

   Note
   The aging time for BPDUs is different from the aging time used by the MAC address table.

Set Bridge Forwarding [D]elay
Sets the waiting period before a bridge changes to a new state, for example, from blocking to forwarding. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The default is 15 seconds.

Spanning Tree [P]ort Configuration
Configures Port Priority, Path Cost, Trunk Priority, and Trunk Path Cost. This procedure is explained in **Configuring STP Port Settings** on page 83.

Configuring STP Port Settings

To configure STP port parameters, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **S** to select Spanning Tree Configuration.
3. From the Spanning Tree Configuration menu, type **P** to select Spanning Tree Port Configuration.

   The STP Port Configuration Menu in Figure 24 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Spanning Tree Configuration->Spanning Tree Port Configuration Menu

Port Trunk   Link    State      Speed  Priority  Path Cost     MAC Address
---- ------- ----  ----------  -----  --------  ---------  -----------------
1     1      Down  Blocking    1000     80   1000:30:AB:00:09:21
2     ---    Up    Forwarding  100      128         4       00:30:AB:00:09:22
3     1      Down  Blocking    1000     80   1000:30:AB:00:09:23
4     1      Down  Blocking    1000     80   1000:30:AB:00:09:24
5     ---    Down  Blocking    10       128         4       00:30:AB:00:09:25
6     ---    Down  Blocking    10       128         4       00:30:AB:00:09:26
7     ---    Down  Blocking    10       128         4       00:30:AB:00:09:27
8     ---    Down  Blocking    10       128         4       00:30:AB:00:09:28
9     ---    Down  Blocking    10       128         4       00:30:AB:00:09:29
10    ---    Down  Blocking    10       128         4       00:30:AB:00:09:2A
11    ---    Down  Blocking    1000     128         4       00:30:AB:00:09:2B
12    ---    Down  Blocking    1000     128         4       00:30:AB:00:09:2C
------------------------------ <COMMAND> ----------------------------------
[S]et Port Priority                      Set [T]runk Priority
Set Path [C]ost                          Set T[r]unk Path Cost
[Q]uit to previous menu


Command>
```

Figure 24 Spanning Tree Port Configuration Menu

4. Adjust the parameter settings as desired. The commands for setting the parameters are described below.

   Set Port Pr[i]ority
   Sets the parameter used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0-255. The default value for priority is 128.

   Note
   Set Port Priority cannot be used on ports that are part of a trunk group.

Set Path [C]ost
Sets the cost parameter used in deciding which port provides the lowest cost path to the root bridge for that LAN. The default value is 4. The range is 1 to 65535.

Set [T]runk Priority
Sets the parameter used as a tie breaker when two or more trunk groups are determined to have equal costs to the root bridge. The default value for priority is 128. The range is 0-255.

Set Trunk Path [C]ost
Sets the cost parameter to decide which trunk group provides the lowest cost path to the root bridge for that LAN. The default values for this parameter are 100 for a 10 Mbps port, 10 for a 100 Mbps port, and 4 for a 1 Gbps port. The range is 1 to 65535.

This following information is for display purposes only and cannot be changed from the Spanning Tree Port Configuration Menu.

Port
The port number.

Trunk
The trunk group number. A number in this column indicates that the port is a member of a port trunk.

Link
The link status between the port and the end node connected to the port. Possible values are:

Up - indicates that a valid link exists between the port and the end node.

Down - indicates that the port and the end node have not established a valid link.

State
This parameter indicates the current STP status of the port. Possible values are:

- ❑ Forwarding
- ❑ Listening
- ❑ Learning
- ❑ Blocking

Speed
The operating speed of the port.

MAC Address
The MAC addresses of the ports on the switch.

Chapter 9
Virtual LANs

This chapter contains basic information about virtual LANs (VLANs). It also contains the procedures for creating, modifying, and deleting VLANs from a local or Telnet management session.

This chapter contains the following sections:

- ❑ **VLAN Overview** on page 87
- ❑ **Tagged and Untagged VLAN Overview** on page 89
- ❑ **Creating a Tagged or Untagged VLAN** on page 93
- ❑ **Viewing or Modifying a Tagged or Untagged VLAN** on page 98
- ❑ **Deleting a Tagged or Untagged VLAN** on page 103
- ❑ **Port-based VLAN Mode Overview** on page 104
- ❑ **Creating a Port-based VLAN** on page 105
- ❑ **Modifying a Port-based VLAN** on page 107
- ❑ **Setting GVRP Status** on page 109
- ❑ **Resetting the VLAN Parameters to Default** on page 110
- ❑ **Setting the VLAN Type** on page 111

VLAN Overview

A VLAN is a group of ports on an Ethernet switch that form a logical Ethernet segment. The ports of a VLAN form an independent broadcast domain where the traffic generated by the nodes of a VLAN remains within the VLAN.

With VLANs, you can segment your network through the switch's management software and so be able to group nodes with related functions into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you could create separate VLANs for the different departments in your company, such as one for Sales and another for Accounting.

VLANs offer several important benefits:

- Improved network performance

  Network performance often suffers as networks grow in size and as data traffic increases. The more nodes on each LAN segment vying for bandwidth, the greater the likelihood overall network performance will decrease.

  VLANs improve network perform because VLAN data traffic stays within the VLAN. The nodes of a VLAN receive traffic only from nodes of the same VLAN. This reduces the need for nodes to handle traffic not destined for them. It also frees up bandwidth within all the logical workgroups.

  Additionally, since each VLAN constitutes a separate broadcast domain, broadcast traffic remains within the VLAN. This too can improve overall network performance.

- Increased security

  Since data traffic generated by a node in a VLAN is restricted only to the other nodes of the same VLAN, VLANs can be used to control the flow of data in your network and prevent data from flowing to unauthorized end nodes.

- Simplified network management

  VLANs can also simplify network management. Before the advent of VLANs, physical changes to the network often had to been made at the switches in the wiring closets. For example, if an employee changed departments, changing the employee's LAN segment assignment might require a change to the wiring at the switches.

But with VLANS, you can change the LAN segment assignment of an end node connected to the switch through the switch's AT-S45 management software. VLAN memberships can be changed any time through the management software without moving the workstations physically, or having to change group memberships by moving cables from one switch port to another.

Additionally, a virtual LAN can span more than one switch. This means that the end nodes of a VLAN do not need to be connected to the same switch and so are not restricted to being in the same physical location.

VLAN Modes

The AT-9410GB switch features two VLAN modes: 802.1Q and port-based. The 802.1Q VLAN mode of the switch complies with the IEEE 802.1Q standard and supports two types of VLANs:

- Untagged VLANs
- Tagged VLANs

Untagged and tagged VLANs are described in the next section. The Port-based VLAN mode is described on page 104.

Tagged and Untagged VLAN Overview

As explained in the **VLAN Overview** section earlier in this chapter, a VLAN consists of a group of ports on one or more Ethernet switches that forms a logical Ethernet segment and an independent broadcast domain. Traffic generated by the end nodes of a VLAN remains within the VLAN and does not cross over to the end nodes of other VLANs unless there is an interconnection device, such as a router or Layer 3 switch.

A VLAN can consist of all the ports on an Ethernet switch, or just a few ports. A VLAN can also span switches and consist of ports from multiple Ethernet switches.

The parts that make up a VLAN are:

- ❑ VLAN name
- ❑ VLAN Identifier
- ❑ Untagged ports
- ❑ Tagged ports
- ❑ Port VLAN Identifier

VLAN Name

Every VLAN in your network should be given a name. The name should reflect the function of the network devices that are be members of the VLAN. Examples include Sales, Production, and Engineering. You will be required to specify a name when you create a VLAN.

VLAN Identifier

Each VLAN in a network must be assigned a number. This number is called the VLAN identifier (VID). This number will uniquely identify each VLAN in your network. You assign the VID number when you create the VLAN.

If a VLAN consists of ports located on only one physical switch in your network, you must assign it a VID unique from all other VLANs in your network.

In instances where a VLAN spans multiple switches, the VID for the VLAN must be the same on each switch where a part of the VLAN resides. This enables the switches to recognize and forward frames belonging to the same VLAN even though the VLAN spans multiple switches.

For example, if you had a VLAN titled Marketing that spanned three AT-9410GB switches, you would assign the Marketing VLAN on each switch the same VID.

Untagged and Tagged Ports

There are two kinds of ports that you can assign to an IEEE 802.1Q-compliant VLAN: tagged ports and untagged ports. The basic different between the two is that an untagged port can be a member of only one VLAN at a time while a tagged port can be a member of multiple VLANs.

Untagged Ports

When the ports on an Ethernet switch are divided into independent VLANs, the switch needs a mechanism for determining which ports belong to which VLANs. For instance, if a switch needs to broadcast a frame to the ports of a particular VLAN, it needs to know which ports comprise the VLAN.

In a VLAN that consists of untagged ports, port membership is determined by what is referred to as the *port VLAN identifier* (PVID). This is a number that you must assign to a port when you assign it as an untagged member of a VLAN. The PVID of a port will be the same as the VID of the VLAN in which the port is to be an untagged member.

Here is an example. Let's assume that you are creating a new VLAN called Sales and that you assigned the VLAN a VID of 4. You have decided that Ports 1 through 4 on the switch will be untagged members of the new VLAN. Consequently, you would assign Ports 1 to 4 PVIDs of 4, same as the VID. Now, when the switch receives a frame on one of the ports on the Sales VLAN and it needs to broadcast the frame to the other ports of the VLAN, it will know that the Sales VLAN consists of Ports 1 to 4.

A VLAN that consists of only untagged ports is referred to as an *untagged VLAN*. In order for frames from untagged VLANs to cross a VLAN boundary, there must be a Layer 3 switch or router providing an interconnection between the VLANs.

You can assign each port only one PVID. Consequently, a port can be an untagged member of only one VLAN at a time.

> **Note**
> The AT-9410GB Switch is pre-configured with one untagged VLAN, called the Default VLAN. All ports on the switch are members of this VLAN. The Default VLAN has a VID of 1. Consequently, all the ports in the VLAN have a PVID value of 1.

The reason the ports are called untagged is because it is assumed that the frames received on this type of port will not to contain any information that indicates VLAN membership, and that VLAN membership will be determined solely by a port's PVID. (This contrasts

with tagged ports, explained next, where VLAN membership is determined by information within the frames themselves.) Frames received on untagged ports and lacking any VLAN identifying information are referred to as *untagged frames*.

When a switch receives a frame on an untagged port, it first examines the PVID of the port on which the frame was received and then adds the PVID to the frame itself. It then examines the destination MAC address of the frame. If the destination address is in the MAC address table and if the switch port where the destination node is located is part of the same VLAN as the port that received the frame, the switch sends the frame out the port to the destination node.

If the destination MAC address is not in the MAC address table, the switch broadcasts the frame to all the ports that share the same PVID as the port that received the frame.

Tagged Ports

The second type of port that can be a member of a VLAN is called a tagged port. There are several principal differences between a tagged port and an untagged port.

As explained earlier, a switch determines the VLAN membership of a frame received on an untagged port by examining the PVID that you assigned to the port.

But when a frame is received on a tagged port, the switch examines the frame itself to determine VLAN membership. The VLAN information within an Ethernet frame is referred to as a *tag* or *tagged header*. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard).

When a switch receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports that share the same VID.

Any network device connected to a tagged port must be IEEE 802.1Q-compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

The principal benefit of tagged ports is that they can belong to more than one VLAN at one time. This can greatly simplify the task of adding shared devices to the network. For example, an IEEE 802.1Q-compliant server can be configured to accept and return packets from many different VLANs simultaneously.

Tagged VLANs are also useful where multiple VLANs span across switches. You can use one port per switch for connecting all VLANs on the switch to another switch.

The IEEE 802.1Q standard deals with how this tagging information is used to forward the traffic throughout the switch. The handling of frames tagged with VIDs coming into a port is straightforward. If the incoming frame's VID tag matches one of the VIDs of a VLAN that the port is a tagged member of, the frame will be accepted and forwarded to the appropriate ports. If the frame's VID does not match any of the VLANs that the port is a member of, the frame will be discarded.

A VLAN that contains only tagged frames or that contains a combination of tagged and untagged ports is referred to as a *tagged VLAN*. And, as explained previously, any device that you connect to a tagged port of a tagged VLAN must be IEEE 802.1Q-compliant.

So how do you indicate which ports are to be tagged and which are to be untagged when you create a VLAN? The rule is straightforward. If you assign a port to only one VLAN, the switch assumes it is to be an untagged port. If you assign a port to more than one VLAN, the switch assumes that the port is to be both a tagged and untagged port.

General Rules to Creating an Untagged or Tagged VLAN

Below are general rules to observe when creating a VLAN.

- ❑ An AT-9410GB switch can support up to 256 tagged and untagged VLANS.
- ❑ Each VLAN must be assigned a unique VID. However, if a particular VLAN spans multiples switches, each part of the VLAN on the different switches must be assigned the same VID.
- ❑ A port can be an untagged member of only one VLAN at a time.
- ❑ A port can be a tagged member of multiple VLANs.
- ❑ You must assign each untagged port a PVID. The PVID must match the VLAN's VID. You must assign this value manually when you create the VLAN.
- ❑ An untagged VLAN that spans multiple switches requires a port on each switch where the VLAN is located to function as an interconnection between the switches where the various parts of the VLAN reside.
- ❑ If there are end nodes in different VLANs that need to communicate with each other, a router or Layer 3 switch is required to interconnect the VLANs.

Creating a Tagged or Untagged VLAN

The procedure for creating a new VLAN is divided into the following phases:

- ❑ Phase 1: Assigning a VID and name and specifying the port members
- ❑ Phase 2: Converting tagged ports into untagged ports

Performing Phase 1 is required whenever you create a new VLAN. Every VLAN must have a name, VID, and, of course, ports. You will need to perform Phase 2 if some or all of the ports of a VLAN will be untagged ports. Ports that you want to function as untagged ports must be converted by changing their PVIDs, as explained in Phase 2.

To create a new VLAN, start by performing the procedure in Phase 1.

Phase 1

This phase assigns a VID and a name to your VLAN, and also designates the VLAN port members.

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.
2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.

   The VLAN Management Menu in Figure 25 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Advanced Switch Configuration -> VLAN Management Menu

VLAN Type : 802.1Q         GVRP Status :Disabled
VLAN ID    VLAN Name                        VLAN Type
-------  --------------------------------  ----------
1          Default VLAN                     Permanent




--------------------------- <COMMAND> -------------------------------

[N]ext Page               [C]reate VLAN      C[o]nfig VLAN Member
[P]revious Page           [D]elete VLAN       [S]et Port Config
[R]eset VLAN to Default   Set [G]VRP Status   Set VLAN [T]ype
[Q]uit to previous menu


Command>
```

Figure 25 VLAN Management Menu

Note
It is a good idea to check the VLAN Type field in the window to make sure it is set to 802.1Q, which happens to be the default. You can create tagged and untagged VLANs only when the switch is operating in the 802.1Q mode. For instructions on how to change the switch's VLAN mode, see **Setting the VLAN Type** on page 111.

3. From the VLAN Management Menu, select **C** for Create VLAN.

   The VLAN Creation Menu in Figure 30 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Advanced Switch Configuration -> VLAN Creation Menu

VLAN Index :
VLAN Name :

Device          Member
--------        ------------------------------------------------------




---------------------------- <COMMAND> -----------------------------

Set VLAN [I]D/[I]ndex                    [S]elect Port Member
Set VLAN [N]ame                          [A]pply
[Q]uit to previous menu



Command>
```

Figure 26 VLAN Creation Menu

4. Type **I** to select Set VLAN ID/Index.

   The following prompt is displayed:

   ```
   Enter VLAN ID ->Enter VLAN ID >
   ```

5. Enter a V ID for the new VLAN. The VID can be between 2 and 4094. Press Enter.

   If this VLAN will be unique in your network, then its VID must also be unique from all other VIDs in the network.

If this VLAN will be part of a larger VLAN that spans multiple switches, than the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that will span three switches, you must assign the Sales VLAN on each of the switches the same VID value.

6. Type **N** to select Set VLAN Name.

   The following prompt is displayed:

   ```
   Enter VLAN Name ->Enter VLAN Name >
   ```

7. Enter a VLAN name of up to 32 characters. Press Enter

   The name should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!).

   If the VLAN will be unique in your network, then the name should be unique as well.

   If the VLAN will be part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

8. Type **S** to choose Select Port Member.

   The following prompt is displayed:

   ```
   Enter port number>
   ```

9. Enter all the ports, both tagged and untagged, that are to be members of the new VLAN. Press Return.

   You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9)

10. Type **A** to select Apply.

    You have now created a new VLAN. You gave it a VID and a name. You also specified which ports are to be members of the new VLAN.

    It is important to note, however, that by default all of the ports that you just added to the new VLAN are tagged ports, meaning they are shared ports. The ports are still members of their current VLANs.

    If you want to convert the ports into untagged ports, you must perform the procedure in Phase 2.

Phase 2 This phase of creating a new VLAN converts the tagged ports that you added to the new VLAN into untagged ports. This involves changing the PVIDs of the ports so that they match the VID of the new VLAN. For example, if you assigned the new VLAN a VID of 4, you must change the PVIDs of the untagged ports to 4. The following procedure explains how this is accomplished.

The following procedure assumes that you are continuing directly from Phase 1.

1. From the VLAN Creation Menu, type **Q** to select Quit to Previous Menu.

   The VLAN Management Menu is displayed again.

2. Type **S** to select Set Port Config.

   The VLAN Port Configuration Menu is displayed. An example is shown in Figure 26.

```
AT-9410GB Local Management System
VLAN Management -> VLAN Port Configuration Menu

Port   PVID
 ----   ----
   1      1
   2      1
   3      1
   4      1
   5      1
   6      1
   7      1
   8      1
-------------------------------- <COMMAND> ------------------------
 [N]ext page                              Set Port [V]ID
 [P]revious Page
 [Q]uit to previous menu


Command> _
Enter the character in square brackets to select option
```

Figure 27 VLAN Port Configuration Menu

This window lists the ports on the switch and each port's current PVID assignment. For example, referring to the figure above, Ports 1 to 8 all have a PVID of 1, meaning that they are untagged members of the Default VLAN, which has a VID of 1.

3. To set a PVID, type **V** to select the Set Port VID option.

The following prompt is displayed:

```
Set PVID->Enter port number>
```

4. Enter the port number whose PVID you want to change.

   A prompt similar to the following is displayed:

   ```
   Enter PVID for port 1>
   ```

5. Enter the new PVID for the port.

   Once a new PVID has been assigned to a port, the port is removed as an untagged port from its current VLAN and added to the new VLAN as an untagged port.

   If the port is also an tagged member of any VLANs, it remains as a tagged member of those VLANs.

6. Repeat Steps 3 to 5 to assign new PVIDs to any other ports that are to be untagged members of the new VLAN.
7. Once you have changed all of the appropriate PVIDs, type **Q** to select Quit to Previous Menu.

   The VLAN Management Menu in Figure 25 on page 93 is displayed again.

This completes the procedure for creating a new VLAN.

Viewing or Modifying a Tagged or Untagged VLAN

There are two phases to modifying a VLAN. You might need to perform both phases or just one, depending on what it is you want to change in the VLAN. The phases are:

- ❑ Phase 1: In this phase, you can view a VLAN's configuration, as well as change a VLAN's name and add or remove tagged ports.
- ❑ Phase 2: In this phase, you can add or remove untagged ports.

Phase 1

This phase explains how to display the Config VLAN Member Menu of a VLAN. This window displays a VLAN's configuration. You can also use the window to change a VLAN's name and add or remove tagged ports.

> **Note**
> If you do not want to change a VLAN's name or add or remove tagged ports, then skip this procedure and go straight to Phase 2 to add or remove untagged ports.

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.
2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.
3. From the VLAN Management Menu, select **O** for the Config VLAN Member option.

   The following prompt is displayed:

   ```
   Enter VLAN ID>
   ```

4. Enter the VID of the VLAN you want to view or modify.

The Config VLAN Member Menu for the VLAN is displayed. This VLAN contains all the current information about the VLAN. An example is shown in Figure 26.

```
AT-9410GB Local Management System
VLAN MAnagement-> Config VLAN Member Menu

VLAN ID: 3 VLAN Name: Engineering

Port            Participation           Tagging
----            -------------           -------
8               Static                  No
9               Static                  No
10              Static                  No
11              Static                  No
16              Static                  No
23              Static                  No

------------------------------Command-----------------------------
[N]ext Page             [C]hange VLAN Name     [A]dd VLAN Member
[P]revious Page         [M]odify Participation [R]emove VLAN Member
[Q]uit to previous menu

Command> _
Enter the character in square brackets to select option
```

Figure 28 Config VLAN Member Menu

The columns in the window are defined below:

Port
This column lists the ports that are members of the VLAN.

Participation
This column indicates whether the port is participating in GVRP. For more information on this selection, refer to **Setting GVRP Status** on page 109.

Tagging
This column indicates whether the port is a tagged or untagged port in the VLAN. No indicates that the port is an untagged member while Yes indicates that it is a tagged member.

5. To modify the VLAN, use the commands at the bottom of the screen.

   The commands are described below:

   [C]hange a VLAN Name
   This command is used to change a VLAN's name. To use the command, type **C** and enter the new name at the command prompt.

[M]odify Participation
This command is explained in the section **Setting GVRP Status** on page 109

[A]dd VLAN Member
This command adds tagged ports to the VLAN. Type **A** and then specify the ports that you want to add as tagged ports to the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9). Press Enter.

Note
To add untagged ports to the VLAN, perform **Phase 2** on page 100.

[R]emove VLAN Member
This command removes tagged ports from the VLAN. Type **R** and specify the tagged ports that you want to remove from the VLAN. Press Enter. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

Note
You cannot use this command to remove untagged ports from a VLAN. To remove untagged ports, perform **Phase 2** below. Furthermore, you cannot use this command to remove a port whose GVRP participation has been set to Forbidden. You must first change the port's GVRP participation to Static, after which you can remove the port from the VLAN.

Phase 2

You perform this phase whenever you need to add or remove an untagged port from a VLAN. This phase explains how to change the PVIDs of the ports so that they match the VID of a different VLAN. For example, if you want to assign Port 2 as an untagged member of a VLAN with a VID of 4, you must change the PVID of the port to 4.

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.
2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.
3. Type **S** to select Set Port Config.

The VLAN Port Configuration Menu is displayed. An example is shown in Figure 26.

```
AT-9410GB Local Management System
VLAN Management -> VLAN Port Configuration Menu


 Port   PVID
 ----   ----
  1      1
  2      1
  3      1
  4      1
  5      2
  6      2
  7      2
  8      2
-------------------------------- <COMMAND> -----------------------
[N]ext page                              Set Port [V]ID
[P]revious Page                          [Q]uit to previous menu

Command> _
Enter the character in square brackets to select option
```

Figure 29 VLAN Port Configuration Menu

This window lists the ports on the switch and each port's current PVID assignment. For example, referring to the figure above, Ports 1 to 4 and Ports 5 to 8 are untagged members of different VLANs.

4. To set a PVID, type **V** to select Set Port VID.

   The following prompt is displayed:

   ```
   Set PVID->Enter port number>
   ```

5. Enter the port number whose PVID you want to change.

   A prompt similar to the following is displayed:

   ```
   Enter PVID for port 1>
   ```

6. Enter the new PVID for the port.

   Once a new PVID has been assigned to a port, the port is removed as an untagged port from its current VLAN and added as an untagged port to the VLAN whose VID matches the PVID.

Note
A port that is a tagged member of another VLAN remains as a tagged member of the VLAN.

7. If necessary, repeat Steps 4 to 6 to assign new PVIDs to other ports.
8. Once you have changed all of the appropriate PVIDs, type **Q** to select Quit to Previous Menu.

   The VLAN Management Menu in Figure 25 on page 93 is displayed again.

This completes the procedure for modifying a VLAN.

Deleting a Tagged or Untagged VLAN

To delete a VLAN, perform the following procedure:

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.
2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.
3. From the VLAN Management Menu, select **D** for Delete VLAN.
4. At the command prompt, enter the VLAN ID of the VLAN you would like to delete. Press Enter.

   The VLAN is removed from the switch. The PVIDs of the untagged ports in the VLAN are changed to 1, making the ports untagged members of the Default VLAN.

> **Note**
> You cannot delete the Default VLAN, which has a VLAN ID of 1.The Default VLAN is a permanent VLAN.

Port-based VLAN Mode Overview

The AT-9410GB switch features a special Port-based VLAN mode. This VLAN mode allows you to create VLANs that are slightly different than the tagged and untagged VLANs described earlier in this chapter.

> **Note**
> For those of you who are familiar with Allied Telesyn products, please note that the port-based VLAN described here is not the same as the port-based VLANs featured in our other managed switches, such as the AT-8024 Fast Ethernet Switch. The untagged VLAN described earlier in this chapter is analogous to the port-based VLAN featured in other Allied Telesyn switch products.

Port-based VLANs are just lists of ports that belong to different VLANs on the switch. To create a port-based VLAN, you simply indicate which ports you want in it. You do not configure PVIDs, as you do for untagged ports, and, while you do specify a unique VID when you create a port-based VLAN, its use is limited to within the switch. A VID is not used across multiple switches to identify different port-based VLANs.

Port-based VLANs do have a couple of advantages over tagged and untagged VLANs described earlier in this chapter. For instance, port-based VLANs are easier to configure, mainly because you do not have to worry about setting PVIDs.

Plus, it can be easier to share network resources. Ports can be shared in port-based VLANs and the shared devices do not need to be IEEE 802.1Q-compliant, as required with a tagged VLAN.

The major disadvantage to port-base VLANs is *VLAN leakage*, where frames that originate in one VLAN end up in another. This can occur where port-based VLANs share ports.

Here is how this can occur. Let's assume that a frame arrives on a switch port that is shared among three different VLANs. If the destination MAC address in the frame has not been learned by the switch, the frame will be broadcast out the ports of all three VLANs. Hence, the frame crosses the boundaries of the VLANs.

This might not be a problem for you if network security is not a major concern. However, if it is a high priority, then either the VLANs that you create with the Port-based VLAN mode should not contain shared ports, or you should instead create tagged VLANs, as described earlier in this chapter.

Creating a Port-based VLAN

To create a new port-based VLAN, perform the following procedure:

> **Note**
> This procedure assumes that the switch is already running in the Port-based VLAN mode. For instructions on how to change the VLAN mode of the switch, refer to **Setting the VLAN Type** on page 111.

1. From the Main Menu, type **A** to select Advanced Switch Configuration Menu.
2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.

   The VLAN Management Menu is displayed.

3. From the VLAN Management Menu, type **C** to select Create VLAN.

   The VLAN Creation Menu in Figure 30 is displayed.

```
AT-9410GB Local Management System

Advanced Switch Configuration -> VLAN Creation Menu

VLAN Index :
VLAN Name :

Port Member
-----------------------------------------------------




---------------------------- <COMMAND> -----------------------------

Set VLAN [I]D/[I]ndex                    [S]elect Port Member
Set VLAN [N]ame                          [A]pply
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

Figure 30 VLAN Creation Menu

4. Type **I** to select Set VLAN ID/Index.

   The following prompt is displayed:

   ```
   Enter VLAN ID ->Enter VLAN ID >
   ```

5. Enter a unique VID for the new VLAN. The VID can be between 2 and 4094. Press Enter.

   Since the switch does not examine the VID in tagged headers of tagged frames when operating in the Port-based VLAN mode, this VID value does not need to be unique from all other VLANs in your network. It only needs to be unique from the other VLANs in the switch on which you are creating the VLAN.

6. Type **N** to select the Set VLAN Name option and enter a VLAN name using 0 to 32 characters.

   The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!). Then press Enter.

7. Type **S** to Select Port Members for the new VLAN.

   You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9)

   The VLAN must include at least one port.

   Note
   The ports that you add to the new VLAN are not removed from their current VLAN assignments. You must remove the ports manually from the other VLANs if you do not want them to be shared. For instructions, refer to **Modifying a Port-based VLAN** on page 107.

8. Type **A** to select Apply. This will save the VLAN you have just created and make it visible in the VLAN Management Menu.

   You can repeat this procedure to create additional port-based VLANs.

Modifying a Port-based VLAN

The following procedure explains how to change the name of a port-based VLAN, as well as add or remove ports.

To modify a port-based VLAN, perform the following procedure:

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.
2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.
3. From the VLAN Management Menu, select **O** for the Config VLAN Member option.

   The following prompt is displayed:

   ```
   Enter VLAN ID>
   ```

4. Enter the VID of the VLAN you want to view or modify.

   The Config VLAN Member Menu for the VLAN is displayed. This VLAN contains all the current information about the VLAN. An example is shown in Figure 26.

```
AT-9410GB Local Management System
VLAN MAnagement-> Config VLAN Member Menu

VLAN ID: 3      VLAN Name: Engineering

Group Members
-----------------------------------------------------
1, 2, 3, 4, 5




------------------------------Command----------------------------
[N]ext Page             [C]hange VLAN Name     [A]dd VLAN Member
[P]revious Page         [M]odify Participation [R]emove VLAN Member
[Q]uit to previous menu

Command> _
Enter the character in square brackets to select option
```

Figure 31 Config VLAN Member Menu

5. To modify the VLAN, use the commands at the bottom of the screen.

   The commands are described below:

   [C]hange a VLAN Name
   This command changes a VLAN's name. Type **C** and enter the new name at the command prompt.

   [M]odify Participation
   This command is disabled when the switch is operating in the port-based VLAN mode.

   [A]dd VLAN Member
   This command adds ports to the VLAN. Type **A** and then specify the ports that you want to add as members of the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9). Press Enter.

   Note
   Any port that you add to a VLAN remains a member of the VLAN(s) in which it is currently assigned. If you do not want the port to be a shared port, you must remove it from the other VLANs.

   [R]emove VLAN Member
   This command removes ports from the VLAN. Type **R** and specify the tagged ports that you want to remove from the VLAN. Press Enter. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

   Note
   You cannot remove a port if it is not already a member of another VLAN.

Setting GVRP Status

Note
Global GVRP is not supported in port-based VLAN mode.

To set the GVRP status, perform the following procedure:

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.
2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.
3. From the VLAN Management Menu, select **G** for Set GVRP Status.

   The following prompt is displayed.

   ```
   Enable or Disable GVRP status (E/D)>
   E for Enable; D for Disable
   ```

4. Type **E** to select Enable.

   The default setting is Disabled.

   The GVRP Status in the VLAN Management Menu is immediately changed to reflect the new setting.

Resetting the VLAN Parameters to Default

This command deletes all VLANs that you created. All ports are returned back to the Default VLAN.

To return the VLAN parameters of the switch to their default settings, perform the following procedure:

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.
2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.
3. From the VLAN Management Menu, select **R** for Reset VLAN to Default.

   The following prompt is displayed.

   ```
   Are you sure you want to reset VLAN configuration to
   factory default (Y/N)>
   Y for Yes; N for No
   ```

4. Type **Y** to select Yes.

   The following prompt is displayed.

   ```
   Are you sure you want to reset VLAN configuration to
   factory default (Y/N)>
   Reset to factory default completed, press any key to
   continue...
   ```

   The default VLAN settings are immediately activated on the switch and displayed in the VLAN Management Menu.

Setting the VLAN Type

The AT-9410GB switch can operate in either the 802.1Q VLAN mode, for creating tagged and untagged VLANs, or the port-based VLAN mode.

Note
The VLAN Type default is 802.1Q.

To change the VLAN mode, perform the following procedure:

1. From the Main Menu, type **A** to select the Advanced Switch Configuration Menu.
2. From the Advanced Switch Configuration Menu, type **V** to select VLAN Management.
3. From the VLAN Management Menu, type **T** to select Set VLAN Type.

   The following prompt is displayed.

   ```
   Set VLAN type (P/8)>
   ```

4. Enter **P** for the Port-based VLAN mode or **8** for the 802.1Q VLAN mode.

Note
Changing the VLAN type setting deletes all tagged and untagged VLANs created in the 802.1Q VLAN mode.

Chapter 10
MAC Address Table

This chapter contains the procedures for viewing the static and dynamic MAC address table. The sections in this chapter include:

- ❑ **MAC Address Overview** on page 113
- ❑ **Displaying MAC Addresses** on page 115
- ❑ **Viewing MAC Addresses by Port** on page 117
- ❑ **Viewing the MAC Addresses by MAC** on page 118
- ❑ **Viewing the MAC Addresses of a VLAN** on page 119
- ❑ **Adding Static MAC Addresses** on page 120
- ❑ **Deleting Static MAC Addresses** on page 121
- ❑ **Changing the Aging Time** on page 122

MAC Address Overview

Every hardware device that you connect to your network has a unique MAC address associated with it. A MAC address is assigned to a device by the device's manufacturer. For example, every network interface card that you use to connect your computers to your network has a MAC address assigned to it by the adapter's manufacturer.

The AT-9410GB Gigabit Ethernet Switch contains a 4 kilobyte MAC address table. The switch uses the table to store the MAC addresses of the network nodes connected to its ports, along with the port number on which each address was learned.

The switch learns the MAC addresses of the end nodes by examining the source address of each packet received on a port. It adds the address and port on which the packet was received to the MAC table if the address has not already been entered in the table. The result is a table that contains all the MAC addresses of the devices that are connected to the switch's ports, and the port number where each address was learned.

When the switch receives a packet, it also examines the destination address and, by referring to its MAC address table, determines the port where the destination node is connected. It then forwards the packet to the appropriate port and on to the end node. This increases network bandwidth by limiting each frame to the appropriate port when the intended end node is located, freeing the other switch ports for receiving and transmitting data.

If the switch receives a packet with a destination address that is not in the MAC address table, it floods the packet to all the ports on the switch. If the ports have been grouped into virtual LANs, the switch floods the packet only to those ports which belong to the same VLAN as the port on which the packet was received. This prevents packets from being forwarded onto inappropriate LAN segments and increases network security. When the destination node responds, the switch adds its MAC address and port number to the table.

If the switch receives a packet with a destination address that is on the same port on which the packet was received, it discards the packet without forwarding it on to any port. Since both the source node and the destination node for the packet are located on the same port on the switch, there is no reason for the switch to forward the packet. This too increases network performance by preventing frames from being forwarded unnecessarily to other network devices.

The type of MAC address described above is referred to as a *dynamic MAC address*. Dynamic MAC addresses are addresses that the switch learns by examining the source MAC addresses of the frames received on the ports.

Dynamic MAC addresses are not stored indefinitely in the MAC address table. The switch deletes a dynamic MAC address from the table if it does not receive any frames from the node over a specified period of time. The switch assumes that the node with that MAC address is no longer active and that its MAC address can be purged from the table. This prevents the MAC address table from becoming filled with addresses of nodes that are no longer active.

The period of time that the switch waits before purging an inactive dynamic MAC address is called the *aging timer*. This value is adjustable on the AT-9410GB Switch. The default value is 300 seconds (5 minutes). For instructions on changing the aging timer, refer to **Changing the Aging Time** on page 122.

The MAC address table can also store *static MAC addresses*. A static MAC address, once entered in the table, remains in the table indefinitely and is never deleted, even when the end node is inactive.

You might need to enter static MAC addresses of end nodes the switch will not learn in its normal dynamic learning process, or if you want a MAC address to remain permanently in the table, even when the end node is inactive.

Displaying MAC Addresses

To display the MAC address table, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database Menu.

   The Forwarding Database Menu in Figure 32 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Advanced Switch Configuration -> Forwarding Database Menu

[S]tatic Address Table
Display MAC Address by [P]ort
Display MAC Address by [M]AC
Display MAC Address by [V]ID
[Q]uit to previous menu



Command>
```

Figure 32 Forwarding Database Menu

3. To display MAC addresses, select from the options below.

   [S]tatic Address Table
   This displays all the static addresses assigned to the ports on the switch.

   Display MAC Address by [P]ort
   This displays all the static and dynamic MAC addresses on a selected port.

   Display MAC Address by [M]AC
   This displays all the static and dynamic MAC addresses on the switch.

   Display MAC Address by [V]ID
   This displays all the MAC addresses of a particular VLAN.

Figure 33 is an example of the Display MAC Address by MAC window, which displays both static and dynamic MAC addresses in numerical order.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Forwarding Database Menu -> Display MAC Address by MAC

Age-Out Time:  300 Sec.

MAC Address          Port
-----------------    ----
00:06:5B:23:0F:7E     3
00:08:C7:73:71:F5     3
00:10:40:00:DC:D7     3
00:10:40:02:00:FE     3
00:12:CD:00:12:23     9
00:30:AB:00:09:20     CPU
00:30:AB:00:09:21     1
00:30:AB:00:09:22     2
00:30:AB:00:09:23     3
00:30:AB:00:09:24     4
-------------------------- <COMMAND> ---------------------------

[N]ext Page                                Set [A]ge-Out time
[P]revious Page                            [Q]uit to previous menu



Command>
```

Figure 33 Display MAC Address by MAC Window

The information is for viewing purposes only, except for the Set Age-Out Time. The columns in the window are defined below.

MAC Address
The MAC address of the node connected to the switch.

Port
The port on the switch where the MAC address was learned.

Set [A]ge-Out Time
This allows you to manually set the MAC aging time. The range is 10 to 1048 seconds. The default setting is 300.

Viewing MAC Addresses by Port

This section contains the procedure for viewing the dynamic MAC addresses that have been learned on a particular port. You can also use this procedure to view any static MAC addresses that have been assigned to a port.

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database Menu.
3. From the Forwarding Database Menu, type **P** to select View MAC Addresses by Port.

   The following prompt is displayed:

   ```
   Enter port number >
   Port number is in range of 1 to 12
   ```

4. Enter the number of the port whose static and dynamic MAC addresses you want to view and press Return.

   A window is displayed with the MAC addresses of the nodes on the port. The columns in the window and the definitions of the columns are the same as for the Display MAC Address by MAC window on page 116.

Viewing the MAC Addresses by MAC

This section contains the procedure for viewing the dynamic MAC addresses learned on the ports of the switch. This procedure will also let you view all static MAC addresses that have been assigned to the ports on the switch.

To view the MAC addresses in numerical order on the switch, perform the following procedure.

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database Menu.
3. From the Forwarding Database Menu, type **M** to select Display MAC Address by MAC.

   The management software displays a window with a list of all static and dynamic MAC addresses of the nodes of all ports. For an example of the window and for definitions of the columns, refer to the Display MAC Address by MAC window on page 116.

Viewing the MAC Addresses of a VLAN

The procedure in this section can be useful if you created VLANs on the switch and want to view the MAC addresses of the nodes of a particular VLAN. (This procedure is not of much value if the switch contains only the Default VLAN, in which case displaying the entire MAC address table, as explained earlier in this chapter, produces the same result.)

> **Note**
> To perform this procedure, you need to know the VID number of the VLAN whose MAC addresses you want to view.

To view the MAC addresses of a VLAN on the switch, perform the following procedure.

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database Menu.
3. From the Forwarding Database menu, type **V** to select Display MAC Address by VID.

   The following prompt is displayed:

   ```
   Enter VLAN ID>
   VLAN ID is in range of 1 to 4094
   ```

4. Enter the VID of the desired VLAN and press Return.

   The management software displays a window with a list of the MAC addresses of the nodes in the VLAN. For an example of the window and for definitions of the columns, refer to the Display MAC Address by MAC window on page 116.

Adding Static MAC Addresses

The management software allows you to assign up to 255 static MAC addresses per port on an AT-9410GB Gigabit Ethernet Switch.

To add a static address to the MAC address table, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database Menu.
3. From the Forwarding Database menu, type **S** to select Static Address Table Menu.
4. From the Static Address Table Menu, type **A** to Add New Entry.

   The following prompt is displayed:

   ```
   Enter MAC Address(xx:xx:xx:xx:xx:xx) >
   ```
5. Enter the static MAC address in the following format:

   ```
   xx:xx:xx:xx:xx:xx
   ```

   Once you have specified the MAC address, the following prompt is displayed:

   ```
   Add new entry->Enter port number >
   Port number is in range of 1 to 12
   ```
6. Enter the port number where the static address is to be assigned.

   Once you have specified the port number, the following prompt is displayed:

   ```
   Add new entry->Enter VLAN ID>
   VLAN ID is in range of 1 to 4094
   ```
7. Enter the VID of the VLAN where the port is a member.

   Once you have specified the VLAN ID, the management software adds the static address to the MAC address table.
8. Repeat steps 4 to 7 to enter additional static MAC addresses.

Deleting Static MAC Addresses

To delete a static MAC address, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database Menu.
3. From the Forwarding Database menu, type **S** to select Static Address Table Menu.
4. From the Static Address Table Menu, type **D** to Delete Entry.

   The following prompt is displayed:

   ```
   Enter MAC Address(xx:xx:xx:xx:xx:xx) >
   ```

5. Enter the static MAC address in the following format:

   ```
   xx:xx:xx:xx:xx:xx
   ```

   Once you have specified the MAC address, the following prompt is displayed:

   ```
   Delete entry->Enter VLAN ID>
   VLAN ID is in range of 1 to 4094
   ```

6. Enter the VID of the VLAN where the port to which the static address was assigned is a member.

   Once you have specified the VLAN ID, the management software deletes the static address from the MAC address table.

7. Repeat steps 4 to 6 to delete additional static MAC addresses.

Changing the Aging Time

The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. When the switch detects that no packets have been received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

The default setting for the aging time is 300 seconds (5 minutes).

To adjust the aging time, perform the following procedure:

> **Note**
> The aging time can be adjusted from the following windows: Display MAC Address by Port, Display MAC Address by MAC, and Display MAC Address by VID.

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **F** to select Forwarding Database Menu.
3. From the Forwarding Database Menu, type **P** to select View MAC Addresses by Port, **M** to select Display MAC Address by MAC, or **V** to select Display MAC Address by VID.
4. Once you have made your selection, type **A** to select MAC Aging Time.

   The following prompt is displayed:

   ```
   Enter your new value ->
   Age-out time is in range of 10 to 1048 Sec
   ```

5. Enter a new value in seconds.

   The aging setting is in range of 10 to 1048 seconds. The default setting is 300 seconds.

   The management software immediately activates the new aging time value on the switch.

Chapter 11
Quality of Service

This chapter contains the procedures for configuring the Quality of Service (QoS) feature of the AT-S45 software. Sections in the chapter include:

- **Quality of Service Overview** on page 124
- **Configuring QoS** on page 125

Quality of Service Overview

The AT-9410GB switch supports QoS as specified in the IEEE 802.1p and 802.1Q standards. QoS can be important in network environments where there are time-critical applications, such as voice transmission or video conferencing, that can be adversely affected by packet transfer delays.

Prior to QoS, network traffic was handled in a best-effort manner. File transfer delays did occur, but were mostly transparent to network users. But with the introduction of time-critical applications, packet transfer delays can prove problematic. For example, transfer delays of voice transmission can result in poor audio quality.

QoS was designed to address this problem. The 802.1p standard outlines eight levels of priority, 0 to 7, with 0 the lowest priority and 7 the highest.

The AT-9410GB switch has two priority queues, 1 (low) and 0 (high). When a tagged packet enters a switch port, the switch responds by placing the packet into one of the two queues according to following assignments:

IEEE 802.1p Traffic Class	AT-9410GB Queue
0	1
1	1
2	1
3	1
4	0
5	0
6	0
7	0

For example, a tagged packet with a priority tag of 6 is placed in the high priority queue, while a packet with a priority tag of 1 is placed in the low priority queue.

These priority-to-queue assignments can be overridden using the AT-S45 management software on a per port basis.

Configuring QoS

To configure QoS for the switch, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.
2. From the Advanced Switch Configuration Menu, type **S** to select Quality of Service Configuration Menu.

   The Quality of Service Configuration Menu is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Advanced Switch Configuration -> Quality of Service Configuration Menu

QoS Status : Disabled

Traffic Class          Queue
-------------     -------------
0                 1
1                 1
2                 1
3                 1
4                 0
5                 0
6                 0                        0 : Highest
7                 0                        1 : Lowest

---------------------------- <COMMAND> ------------------------------

Set [S]tatus
Set [P]riority Queue
[Q]uit to previous menu


Command>
```

Figure 34 Quality of Service Configuration Menu

3. From the Quality of Service Configuration Menu, type **S** to select Set Status.

   The following prompt is displayed.

   ```
   Enable or Disable QoS (E/D) >
   E for Enable; D for Disable
   ```

4. Type **E** to enable the service or D to disable it. The default setting is disabled.

5. If you activate QoS and want to change the queue assignments, type **P** to select Set Priority Queue.

   The following prompt is displayed.

   ```
   Enter Traffic Class
   Traffic class is in range of 0 to 7
   ```

   Note
   The default setting for traffic classes 0 - 3 is the low priority queue. The default setting for traffic classes 4 - 7 is the high priority queue.

6. Enter a traffic class.

   The following prompt is displayed.

   ```
   Enter queue for traffic class>
   Queue is in range of 0 to 1
   ```

7. Enter a priority queue (0 - high: 1 - low).

   All tagged frames will be directed to either the low or high priority queue as specified in this step.

   Note
   The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame leaves a switch with the same priority level that it had when it entered.

Chapter 12
IGMP Snooping

This chapter explains how to activate and configure the IGMP snooping feature on the switch. Sections in the chapter include:

- **IGMP Snooping Overview** on page 129
- **Activating IGMP Snooping** on page 130
- **Viewing Group Members** on page 132

IGMP Snooping Overview

The Internet Group Management Protocol (IGMP) enables routers to create lists of nodes that are members of multicast groups. (A multicast group is a group of end nodes that want to receive multicast packets from a multicast application.) The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports. A node wanting to become a member of a particular multicast group responds to a query by sending a report. Nodes that join a multicast group are referred to as *host nodes*.

Once the router has received a report, it notes the multicast group that the host node wants to join and the port on the router where the node is located. Any multicast packets belonging to that multicast group are then forwarded by the router out the port. If a particular port on the router has no nodes that want to be members of multicast groups, the router does not send multicast packets out the port. This improves network performance by restricting multicast packets only to router ports where host nodes are located.

The IGMP snooping feature enables the switch to monitor the flow of queries from the router and reports from the host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to switch ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by further restricting the flow of multicast packets only to those switch ports connected to host nodes.

Without IGMP snooping, the switch would flood all multicast packets out all of its ports, except the port on which it received the packet. Such flooding of packets can negatively impact switch and network performance.

Note
By default, IGMP snooping is disabled on the switch.

Note
The AT-S45 software supports both IGMP version 1 and version 2.

Activating IGMP Snooping

To enable or disable IGMP snooping on the switch and to configure IGMP snooping parameters, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.
2. From the Advanced Switch Configuration Menu, type **I** to select IGMP Snooping Configuration Menu.

   The IGMP Snooping Configuration Menu in Figure 35 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Advanced Switch Configuration -> IGMP Configuration Menu

IGMP Snooping Status:         Disabled
IGMP Snooping Age-Out Timer : 280 seconds.

VLAN ID  Multicast group address
-------  ----------------------




--------------------------- <COMMAND> --------------------------------
[N]ext Page                           [E]nable/Disable IGMP Snooping
[P]revious Page                       [S]et Age Out Timer
[V]iew group members                  [Q]uit to previous menu


Command>
```

Figure 35 IGMP Snooping Configuration Menu

The fields and commands in the window are defined below:

[E]nable/Disable IGMP Snooping
Enables and disables IGMP snooping on the switch. After selecting this option, type **E** to enable or **D** to disable this feature.

[S]et Age Out Timer
Specifies the time period in seconds after which the switch stops sending out multicast packets out a port with an inactive host node. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 280 to 420 seconds. The default is 280 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.

VLAN ID
Specifies the VLAN's ID configured on the switch.

Multicast Group Address
Specifies the IP multicast addresses the switch has learned. The switch can learn up to 128 multicast addresses.

Viewing Group Members

You can use the AT-S45 software to list the ports on the switch with host nodes of each multicast group. To display the list, perform the following procedure:

1. From the Main Menu, type **A** to select Advanced Switch Configuration.
2. From the Advanced Switch Configuration Menu, type **I** to select IGMP Snooping Configuration Menu.
3. From the IGMP Snooping Configuration window, type **V** to select View Group Members.

   The following prompt is displayed:

   ```
   Enter VLAN ID>
   ```

4. Enter the VLAN ID number.

   The following prompt is displayed:

   ```
   Enter IP address>
   ```

5. Enter a multicast address.

   The View Group Members Menu in Figure 36 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

IGMP Configuration Menu -> View Group Members Menu

VLAN ID:     3      Multicast group address:  224.0.1.22
Group members
-------------------------------------------------------------------
3




------------------------------ <COMMAND> ------------------------------

[Q]uit to previous menu


Command>
```

Figure 36 View Group Members Menu

The information in this window is for viewing purposes only. The columns are defined below:

Multicast Group Address
The multicast address of the group.

Group Members
The port(s) on the switch to which one or more host nodes of the multicast group are connected.

VLAN ID
Specifies the VLAN's ID configured on the switch.

Chapter 13
Storm Control Configuration

This chapter contains the procedures for configuring the storm control feature of the AT-S45 management software. Sections in the chapter include:

- **Storm Control Overview** on page 136
- **Activating Broadcast Storm Control** on page 137

Storm Control Overview

Most frames on an Ethernet network are unicast frames. A node sending a unicast frame intends the frame for a particular node on the network. For example, when a node needs to send a file to a network server for storage, the node sends the file in unicast Ethernet frames containing the destination address of the server where the file is to be stored.

Broadcast frames are different. When a node sends out a broadcast frame, the frame is directed to all nodes on the network or all nodes within a particular virtual LAN. Broadcast packets can perform a variety of functions in an Ethernet network. For example, some network operating systems use broadcast frames to announce the presence of devices on the network.

The problem with broadcast frames is that too many of them traversing the network can impact network performance. Should the performance of your network has been diminished by heavy broadcast traffic, you can use the AT-S45 management software to limit the number of broadcast frames passing through the switch and so limit the number of broadcast frames on your network.

In order to use this feature, you must enable the broadcast storm control and set the threshold level.

Note
The AT-S45 default setting is no broadcast frame control on the switch.

Activating Broadcast Storm Control

To activate the Broadcast Storm control feature, perform the following procedure:

1. From the Main Menu, type **B** to select Basic Switch Configuration.
2. From the Basic Switch Configuration Menu, type **C** to select Storm Control Configuration Menu.

   The Broadcast Storm Control window in Figure 37 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Basic Switch Configuration -> Storm Configuration Menu

Broadcast Storm Status: Enabled

Threshold :  Low

----------------------------- <COMMAND> -----------------------------

Set [B]roadcast Status
Set [T]hreshold
[Q]uit to previous menu




Command>
```

Figure 37 Broadcast Storm Control Window

3. Type **B** to Select Set the Broadcast Status.

   The following prompt is displayed:

   ```
   Enable or Disable Broadcast Storm Control (E/D)>
   ```

4. Type **E** to enable Broadcast Storm Control or **D** to disable it. The default setting is disabled.
5. If you enabled Broadcast Storm Control, type **T** to set Threshold.

   The following prompt is displayed:

   ```
   Enter Threshold Level >
   ```

   The values available for the threshold level are:

   - ❑ Low (1000 64-byte packets per second)
   - ❑ Medium (2000 64-byte packets per second)

- ❑ High (5000 64-byte packets per second)

The default threshold level is Low.

6. Enter a threshold level.

Your changes are activated immediately on the switch.

Chapter 14
Port Statistics

This chapter contains the procedure for displaying data traffic statistics. The chapter contains the following section:

- **Displaying Port Statistics** on page 140

Displaying Port Statistics

To display Ethernet port statistics, perform the following procedure:

1. From the Main Menu, type **S** to select Statistics.

   The Statistics menu in Figure 38 is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Main Menu -> Statistics Menu
Port: 1    Elapsed Time Since System Up: 000:00:03:01
<Counter Name>      <Total>                  <Avg./s>
Total RX Bytes      0                        0
Total RX Pkts       0                        0
Good Broadcast      0                        0
Good Multicast      0                        0
CRC/Align Errors    0                        0
Undersize Pkts      0                        0
Oversize Pkts       0                        0
Fragments           0                        0
Jabbers             0                        0
Collisions          0                        0
64-Byte Pkts        0                        0
65-127 Pkts         0                        0
128-255 Pkts        0                        0
256-511 Pkts        0                        0
512-1023 Pkts       0                        0
1024-1518 Pkts      0                        0
---------------------- <COMMAND> --------------------
[S]elect/[N]ext/[P]rev. Port  Since [r]eset  S[t]op refresh [Q]uit



Command>
```

Figure 38 Ethernet Statistics Menu

   By default, the window displays the statistics for port 1.

2. From the Statistics menu, type **S** to select a port.

   The following prompt is displayed:

   ```
   Select port number>
   ```

3. Enter the number of the port whose statistics you want to view. Press Return.

   The information in the window is for viewing purposes only. The statistics are defined below:

   Total RX Bytes
   Number of bytes received on the port.

Total RX Packets
Number of packets received on the port.

Good Broadcast
Number of valid broadcast packets received on the port.

Good Multicast
Number of valid multicast packets received on the port.

CRC/Align Errors
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Undersize Packets
Number of packets that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Oversize Packets
Number of packets exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Fragments
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.

Jabbers
Number of electrical signal errors detected on the port.

Collisions
Number of packet collisions on the port.

64-Byte Pkts
Number of 64-byte packets sent or received by the port. The minimum length of an Ethernet packet is 64 bytes.

65-127 Pkts
Number of 65- to 127-byte packets sent or received by the port.

128-255 Pkts
Number of 128- to 255-byte packets sent or received by the port.

256-511 Pkts
Number of 256- to 511-byte packets sent or received by the port.

512-1023 Pkts
Number of 512- to 1023-byte packets sent or received by the port.

1023-1518 Pkts
Number of 1023- to 1518-byte packets sent or received by the port. The maximum length of an Ethernet packet is 1518 bytes.)

If you want to clear the counters on the port and return them to "0", select the option "R - Reset" from the Port Statistics Menu.

Chapter 15
Management Software Updates

This chapter explains how to obtain new versions of the AT-S45 management software and how to download the software onto an AT-9410GB switch.

You can download new management software onto a switch using either of the following methods:

- Local management session
- Trivial File Transfer Protocol

Sections in the chapter include:

- **Obtaining Software Updates** on page 144
- **Downloading New Management Software from a Local Management Session** on page 145
- **Downloading a New Management Software Image Using TFTP** on page 148

Obtaining Software Updates

New releases of the AT-S45 management software are available from the Allied Telesyn web site at www.alliedtelesyn.com and from our FTP server at ftp.alliedtelesyn.com. To log on to the FTP server, enter "anonymous" for the user name and your email address for the password. Management software for the AT-9410GB switch will have "S45" as part of the filename.

Downloading New Management Software from a Local Management Session

This section contains the procedure for downloading a new version of AT-S45 management software onto a switch from a local management session. The procedure takes approximately 12 minutes to complete.

Note
You cannot perform this procedure from a Telnet or web browser management session.

Caution
The switch will not forward Ethernet traffic during the software download and initialization process.

Note
The current configuration of the switch (e.g., IP address, subnet mask, and virtual LANs) is maintained when you install a new software image on the switch. To return a switch to its default configuration, refer to **Activating the AT-S45 Management Software Default Values** on page 40.

This procedure assumes that you have already obtained the new version of management software and have stored it on the computer from which you will be performing this procedure.

To download a new software onto an AT-9410GB switch, perform the following procedure:

1. Establish a local management session on the switch where you intend to download the new management software.

   For instructions, refer to **Starting a Local Management Session** on page 27.
2. From the Main Menu, type **T** to select Switch Tools Configuration Menu.
3. From the Switch Tools Configuration menu, type **U** to select Software Upgrade Menu.
4. From the Software Upgrade menu, type **X** for XModem Software Upgrade.

The XModem Software Upgrade Menu is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Software Upgrade -> XModem Software Upgrade Menu

Image Version/Date:   1.00E/Jan 15 2002 19:48:12

Baud Rate :           9600bps
Image File Name:
Image File Type:      Binary

------------------------ <COMMAND> -----------------------

[U]pgrade Image and Reboot
[Q]uit to previous menu



Command>
```

Figure 39 XModem Software Upgrade Menu

5. Type **U** to select Upgrade Image and Reboot.

   The following prompt is displayed:

   ```
   Download file (Y/N)>
   ```

6. To continue with the procedure, type **Y** for Yes. To cancel the procedure, type **N** for No.

   If you select to continue, go to the next step.

7. Begin the file transfer. Steps 8 through 11 illustrate how to perform the transfer using the Hilgraeve HyperTerminal program.

8. From the HyperTerminal window, select **Transfer** from the menu. Then select **Send File** from the pull-down menu.

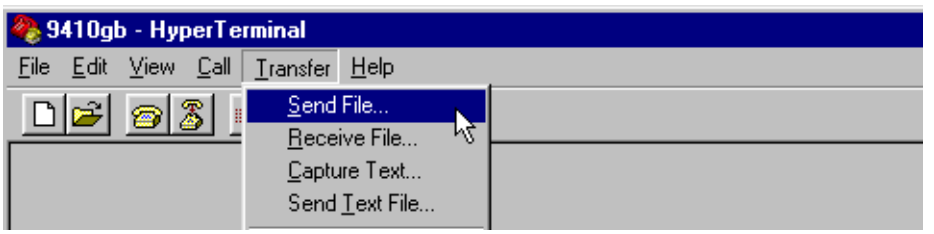

Figure 40 Hilgraeve HyperTerminal Window

The Send File pop-up window is displayed.

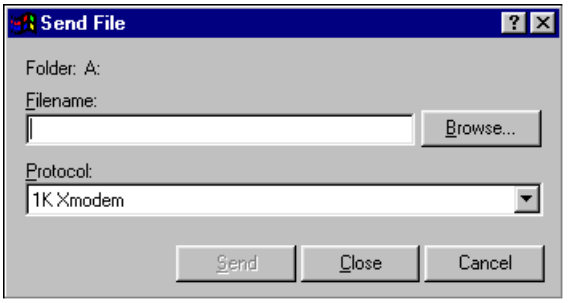

Figure 41 Send File Window

9. Click the **Browse** button on the Send File window to specify the location of the switch's image file.
10. Click on the **Protocol** field and set to 1K Xmodem transfer protocol.
11. Click **Send**.

    The software immediately begins to download onto the switch's CPU. As this process begins, the Xmodem File Send window displays the current status of the software download. This process will take approximately 12 minutes to complete.

    The XModem File Send window is displayed.

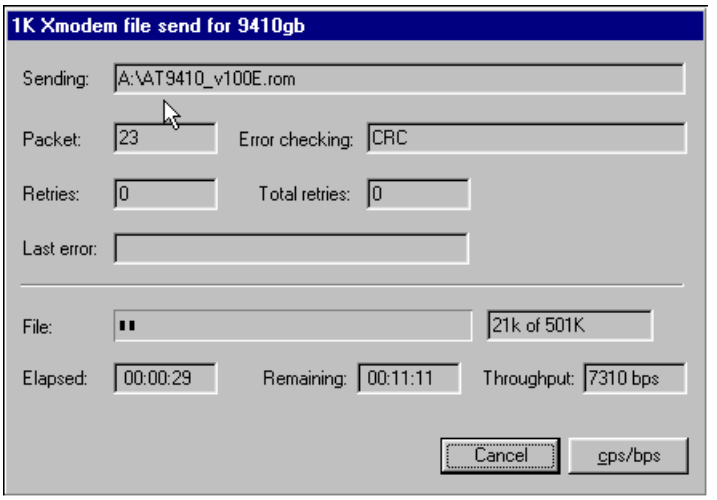

Figure 42 XModem File Send Window

Once the new software download process has completed, the switch begins to initialize the software. This takes approximately 1 minute to complete. Once the initialization process is complete, the switch will automatically reboot.

Note
Do not interrupt the initialization process.

Downloading a New Management Software Image Using TFTP

TFTP software is available from various sources and is included in SNMP which can be purchased through Allied Telesyn. A command line version is included in most UNIX variants and in Windows NT. Please consult the documentation or the manufacturer of the software used on the proper use of the software.

You will need to provide the following information when using the TFTP client software to download the AT-S45 software image:

- ❑ Set TFTP Server IP Address
- ❑ Set Image File Name
- ❑ Upgrade Image and Reboot
- ❑ Set Retry Count

This procedure assumes that you have already obtained a copy of TFTP software and have stored it on the computer from which you will be performing this procedure.

To download the new AS-45 software image onto your AT-9410GB switch, perform the following procedure:

1. Establish a local management session on the switch where you intend to download the new management software.

   For instructions, refer to **Starting a Local Management Session** on page 27.
2. From the Main Menu, type **T** to select Switch Tools Configuration Menu.
3. From the Switch Tools Configuration menu, type **U** to select Software Upgrade Menu.
4. From the Software Upgrade menu, type **T** for TFTP Software Upgrade.

The TFTP Software Upgrade Menu is displayed.

```
AT-9410GB Local Management System
Enter the character in square brackets to select option

Main Menu -> Software Upgrade Menu

Image Version/Date:   1.00E/Jan 15 2002 19:48:12

TFTP Server IP:       149.35.19.3
Image File Name:      AT9410_v100E.rom
Retry Count:          5

---------------------- <COMMAND> -------------------------

Set TFTP [S]erver IP Address
Set Image [F]ile Name
[U]pgrade Image and Reboot
Set [R]etry Count
[Q]uit to previous menu



Command>
```

Figure 43 TFTP Software Upgrade Menu

You will need to provide the following information when using the TFTP client software to download the AT-S45 software image. The options in the window are defined below.

Set TFTP [S]erver IP Address
Sets the IP address of the server which holds the image file.

Set Image [F]ile Name
Sets the path and filename of the software that is to be downloaded onto the switch. The filename of the software should be "ATS45.img". If necessary, change the filename of the image.

[U]pgrade Image and Reboot
Upgrades the new image to your switch and reboots the switch.

Note
Do not begin the upgrade until you have configured the TFTP client.

Set [R]etry Count
The amount of times your system will try to download the image using FTP. The Set Retry Count range is 1 - 20. The default setting is 5.

5. Open a TFTP client to download the software image onto the switch.

   Once the TFTP software is opened, it immediately begins to listen for incoming requests and the syslog server is running.

   Steps 5 and 6 illustrate how to perform the transfer using the Tftpd32 by Ph. Jounin program.

6. Using the TFTP client, select the current directory where the software image is located.

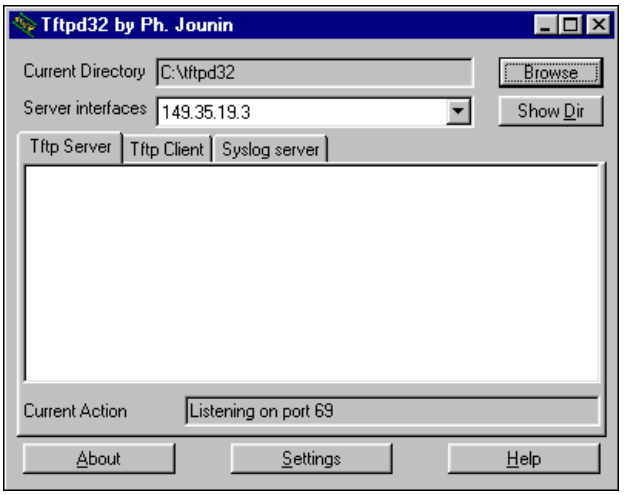

Figure 44 TFTP client software window

7. Return to the local management software upgrade menu as displayed in Figure 43.
8. Type **U** to select Upgrade Image and Reboot.

   The following prompt is displayed:

   ```
   Download file (Y/N)>
   ```

9. Type **Y** to select Yes.

   The software immediately begins to download onto the switch's CPU. This process will take seconds to complete.

   Once the new software download process has completed, the switch begins to initialize the software. This takes approximately 1 minute to complete. Once the initialization process is complete, the switch will automatically reboot.

Section III

Web Browser Management

The chapters in this section explain how to manage an AT-9410GB Gigabit Ethernet switch using a web browser. The chapters include:

- **Chapter 16, Starting a Web Browser Management Session** on page 154
- **Chapter 17, Basic Switch Parameters** on page 157
- **Chapter 18, Port Parameters** on page 176
- **Chapter 19, Port Security** on page 185
- **Chapter 20, Port Trunks** on page 189
- **Chapter 21, Port Monitoring** on page 192**,**
- **Chapter 22, Spanning Tree Protocol** on page 195
- **Chapter 23, Virtual LANs** on page 201
- **Chapter 24, MAC Address Table** on page 220
- **Chapter 25, Quality of Service** on page 228
- **Chapter 26, IGMP Snooping** on page 232
- **Chapter 27, Storm Control Configuration** on page 236
- **Chapter 28, Management Software Updates** on page 239

Chapter 16
Starting a Web Browser Management Session

This chapter contains the procedure for starting a management session on an AT-9410GB Gigabit Ethernet Switch using a web browser, such as Microsoft Internet Explorer or Netscape Navigator.

Starting a Web Browser Management Session

This section explains how to start a web browser management session.

> **Note**
> In order for you to manage an AT-9410GB switch using a web browser, the switch must have an IP address. Initially assigning an IP address to a switch can only be done through a local management session. For instructions, refer to **Configuring an IP Address** on page 32.

To start a web browser management session, perform the following procedure:

1. Start your web browser.

> **Note**
> If your PC with the web browser is connected directly to the switch to be managed or is on the same side of a firewall as the switch, you must configure your browser's network options not to use proxies. Consult your web browser's documentation on how to configure the switch's web browser not to use proxies.

2. Enter the IP address of the switch you want to manage in the URL field of the browser, as shown in Figure 45.

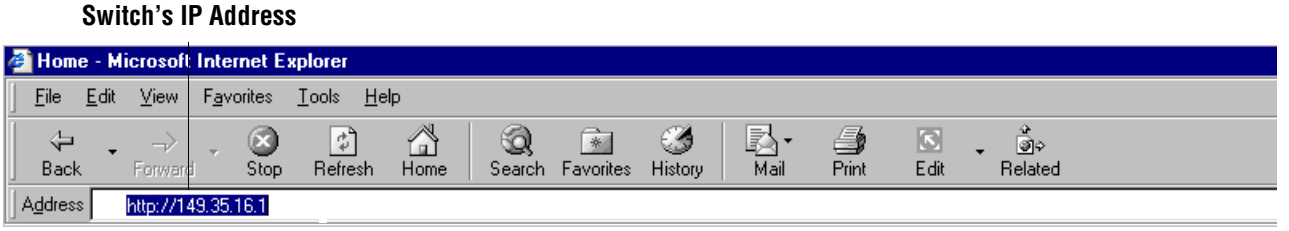
Switch's IP Address
Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Related
Address http://149.35.16.1

Figure 45 Entering a Switch's IP Address in the URL Field

3. When prompted, enter the user name and password. The default user name and password is "manager" and both are case-sensitive.

   On a web management session, the user name and password cannot be changed. To change the user name and password, refer to the local management procedure **Configuring an IP Address** on page 158.

The window shown in Figure 46 is displayed.

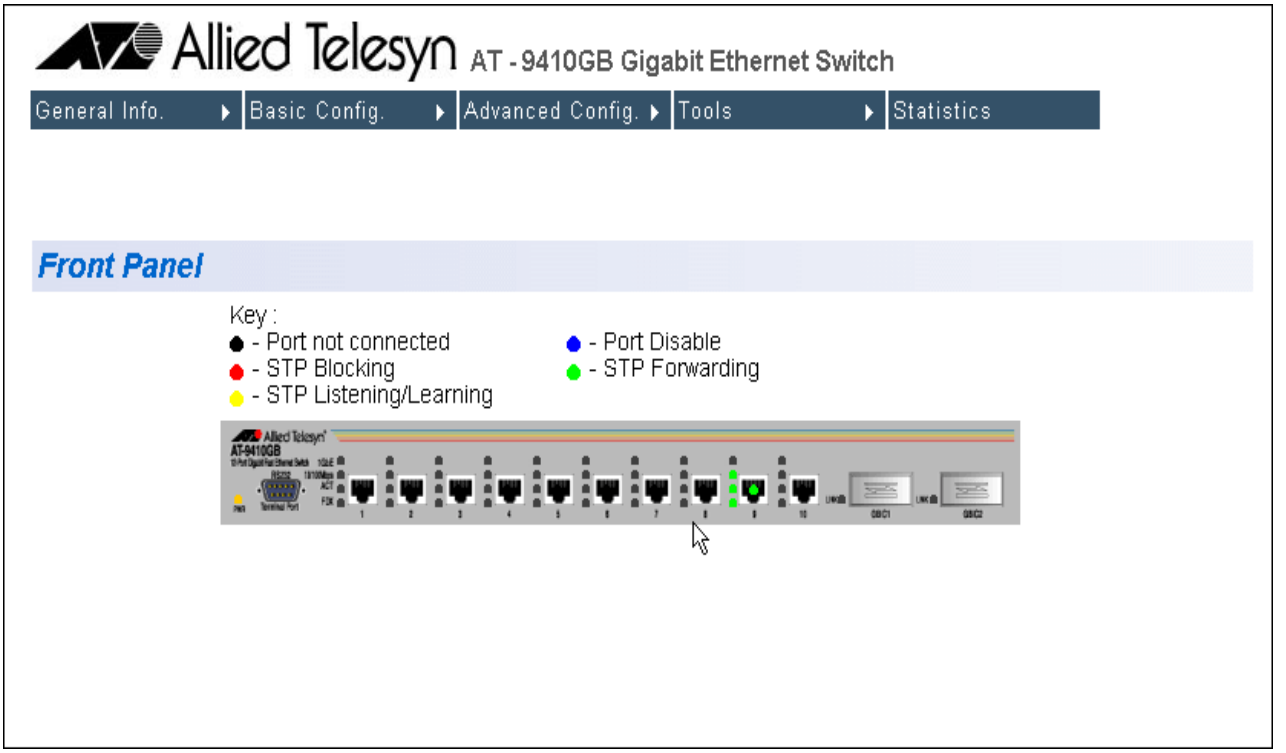

Figure 46 Home Page

This is the Home page of the management software. In the top portion of the Home page is the main menu:

- ❑ General Info.
- ❑ Basic Config.
- ❑ Advanced Config.
- ❑ Tools
- ❑ Statistics

Note
A web browser management session remains active even if you link to other sites. You can return to the management web pages anytime as long as you do not quit the browser.

Browser Tools

You can use the browser tools to move around the Omega menus. Selecting **Back** on your browser's toolbar returns you to the previous display. You can also use the browser's **bookmark** feature on frequently-used Omega menus and windows.

Quitting from a Web Browser Management Session

To exit from a web browser management session, close the web browser.

Chapter 17
Basic Switch Parameters

The procedure in this chapter explains how to set the following switch parameters:

- ❑ **Configuring an IP Address** on page 158
- ❑ **Configuring System Administration Information** on page 160
- ❑ **Setting the User Interface Configuration** on page 162
- ❑ **Activating DHCP** on page 164
- ❑ **Configuring the SNMP Parameters and Trap IP Addresses** on page 166
- ❑ **Resetting a Switch** on page 168
- ❑ **Viewing the AT-S45 Version Number and Switch MAC Address** on page 170
- ❑ **Pinging a Network Device** on page 172
- ❑ **Bootstrap Configuration** on page 174

Configuring an IP Address

Note
For guidelines on when to assign an IP address, subnet address, and gateway address to an AT-9410GB switch, refer to **When Does an AT-9410GB Switch Need an IP Address?** on page 31.

To set the IP address on an AT-9410GB Gigabit Ethernet switch, perform the following procedure:

1. From the Home Page, select **Basic Config**. and then select **IP. Config**. from the sub-menu.

   The IP Configuration menu in Figure 47 is displayed.

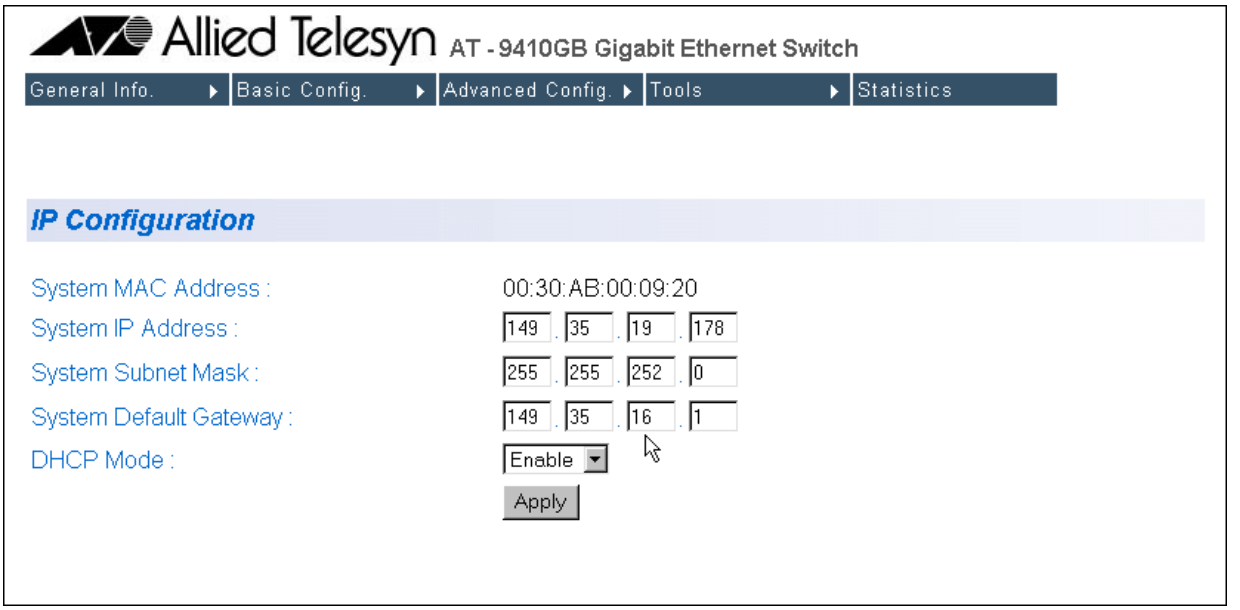

Figure 47 IP Configuration menu

2. Change the parameters as desired.

   The parameters are described below:

   System MAC Address
   This parameter specifies the MAC address of the switch. This parameter cannot be changed.

   System IP address
   This parameter specifies the IP address of the switch. You must specify an IP address if you intend to remotely manage the switch using a web browser, a Telnet utility, or an SNMP management program.

System Subnet Mask
This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch.

System Default Gateway
This parameter specifies the default router's IP address. This address is required if you intend to remotely manage the switch from a management station that is separated from the switch by a router.

DHCP Mode
This parameter specifies the DHCP mode of the switch. You can enable or disable the DHCP mode. The default setting is set to disabled. For background information on DHCP, refer to **Activating the DHCP Service** on page 36.

3. After you have set the parameters, click Apply. Your changes are not stored to flash in the switch until you select Apply.

4. If you made a change to the IP address, subnet mask, or gateway address, you must reset the switch to activate your change. To reset a switch from a web browser management session, refer to **Resetting a Switch** on page 168.

Configuring System Administration Information

To set the switch name for an AT-9410GB Gigabit Ethernet switch, perform the following procedure:

1. From the Home Page, select **Basic Config**. and then select **Admin. Config**. from the sub-menu.

   The Administration Configuration menu in Figure 48 is displayed.

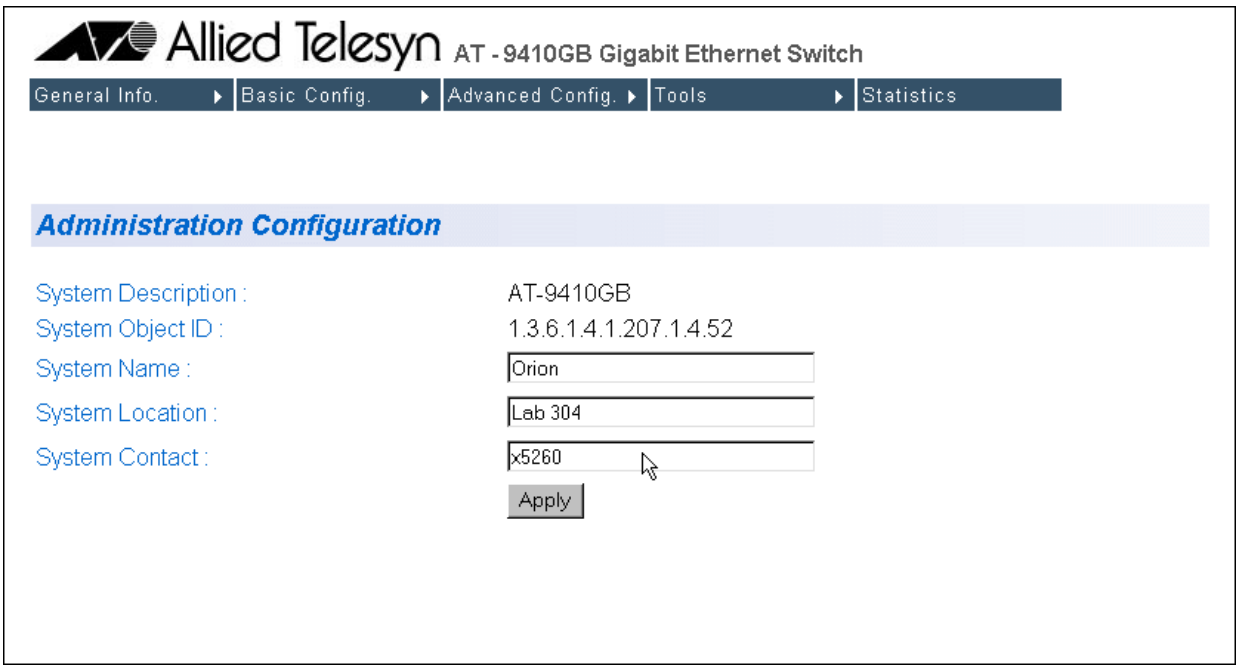

Figure 48 Administration Configuration menu

2. Change the parameters as desired.

   The parameters are described below:

   System Description
   This parameter specifies the model name of the switch. This parameter cannot be changed.

   System Object ID
   This parameter specifies the numeric ID of the switch. This parameter cannot be changed.

   System Name
   This parameter specifies a name for the switch (for example, Sales Ethernet switch). Entering a value for this parameter is optional.

Note
You should assign each switch a name. The names can help you identify the various switches in your network. This can help you avoid performing a configuration procedure on the wrong switch.

System Location
This parameter specifies the location of the switch. Entering a value for this parameter is optional.

System Contact
This parameter specifies the name of the network administrator responsible for managing the switch. Entering a value for this parameter is optional.

3. After you have set the parameters, click Apply. Your changes are not activated until you select Apply.

Setting the User Interface Configuration

The procedure in this section explains how to set the user interface security features of the switch, including idle timeouts, how to enable and disable the different management session options, and how to change the user name and password for the switch.

To set a switch's user interface configuration, perform the following procedure:

1. From the Home Page, select **Basic Config**. and then select **User Interface** from the sub-menu.

   The User Interface page in Figure 49 is displayed.

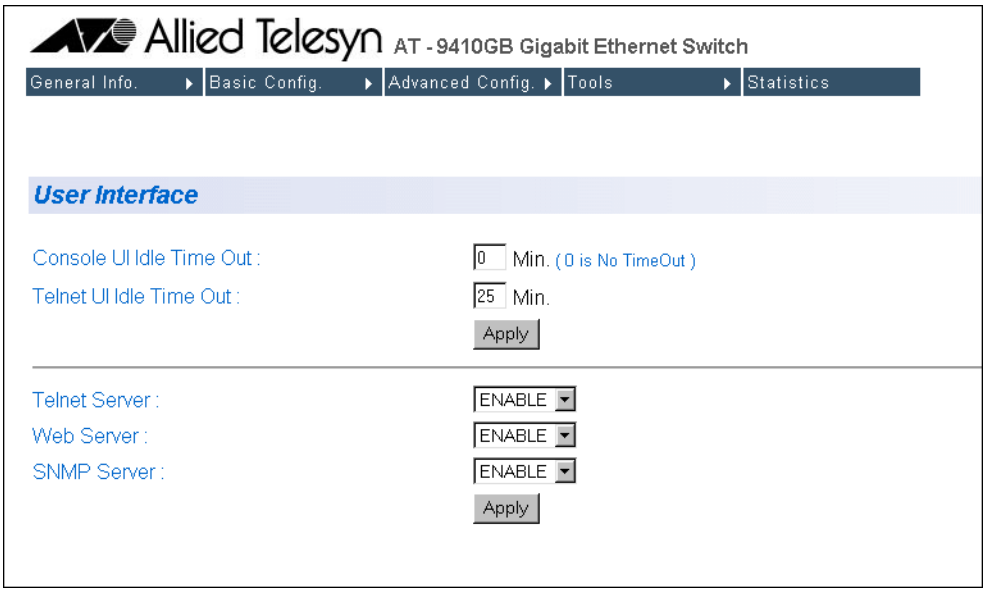

Figure 49 User Interface

2. Change the parameters as desired.

   The parameters in the User Interface Configuration window are described below:

   Console UI Idle Timeout
   This parameter causes the management software to automatically end a management session if it does not detect any activity from the local management station after the specified period of time. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a switch. The default for the console timeout value is 5 minutes.You can set the timeout for between 0 and 60 minutes.

Telnet UI Idle Timeout
This parameter causes the management software to automatically end a management session if it does not detect any activity from the remote management station after the specified period of time. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a switch. The default for the Telnet timeout value is 5 minutes. You can set the timeout for between 0 and 60 minutes.

Enable/Disable Telnet Server
You can disable the Telnet management feature on the switch, and so prevent individuals from managing the switch remotely using a Telnet session.

Enable/Disable SNMP Agent
You can disable the SNMP management feature on the switch, and so prevent individuals from managing the switch remotely using an SNMP agent.

Enable/Disable Web Server
You can disable the Web browser management feature on the switch, and so prevent individuals from managing the switch remotely using a Web browser.

Activating DHCP

This application protocol was developed to simplify network management. It is used to automatically assign IP configuration information to the devices on your network, such as an IP address, subnet mask, and, in some instances, a default gateway address.

The AT-9410GB Gigabit Ethernet switch supports this protocol and can obtain its IP configuration information from a DHCP server on your network. If you activate this feature, the switch will seek its IP address, subnet mask, and default gateway from a DHCP server residing on your network.

Most DHCP services allow you to specify whether the IP address assignment from the server is to be static or dynamic. If you choose static, the server will always assign the same IP address to the switch when the switch is reset or powered on. If you choose dynamic, the server will assign an unused IP address from its list of potential IP addresses each time the switch is reset or powered on.

Note
The DHCP option is disabled by default on the switch.

To activate or deactivate the DHCP protocols on the switch, perform the following procedure:

1. From the Home Page, select **Basic Config**. and then select **IP Config**. from the sub-menu.

   The IP Configuration page in Figure 49 is displayed.

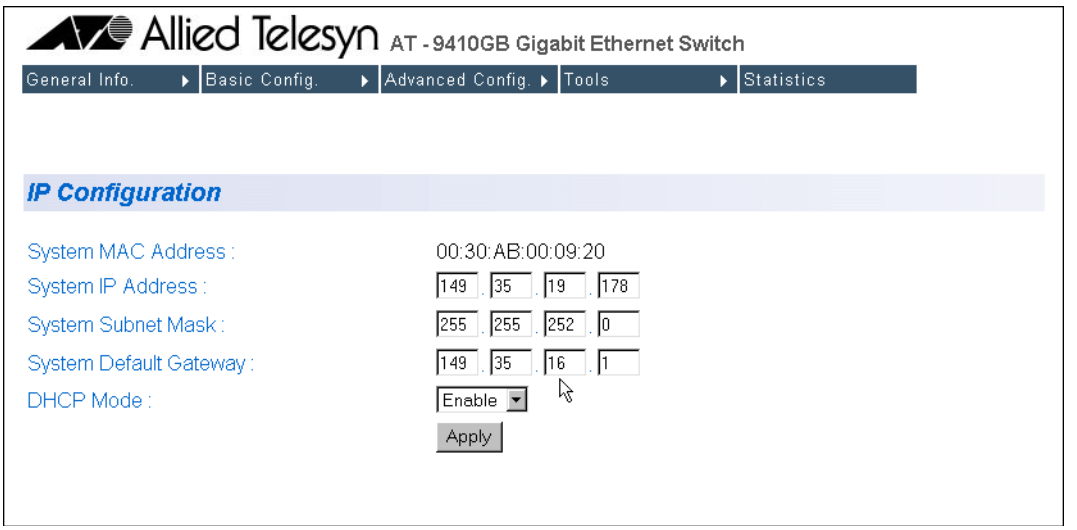

Figure 50 IP Configuration

2. Click on the DHCP Mode pull-down menu, select Enable.
3. Click the **Apply** button.

Configuring the SNMP Parameters and Trap IP Addresses

To change the switch's SNMP community strings or to specify the IP addresses of management stations to receive traps from the switch, perform the following procedure:

1. From the Home page, select **Basic Config.** and then select **SNMP Config.** from the sub-menu.

   The SNMP Configuration page in Figure 51 is displayed.

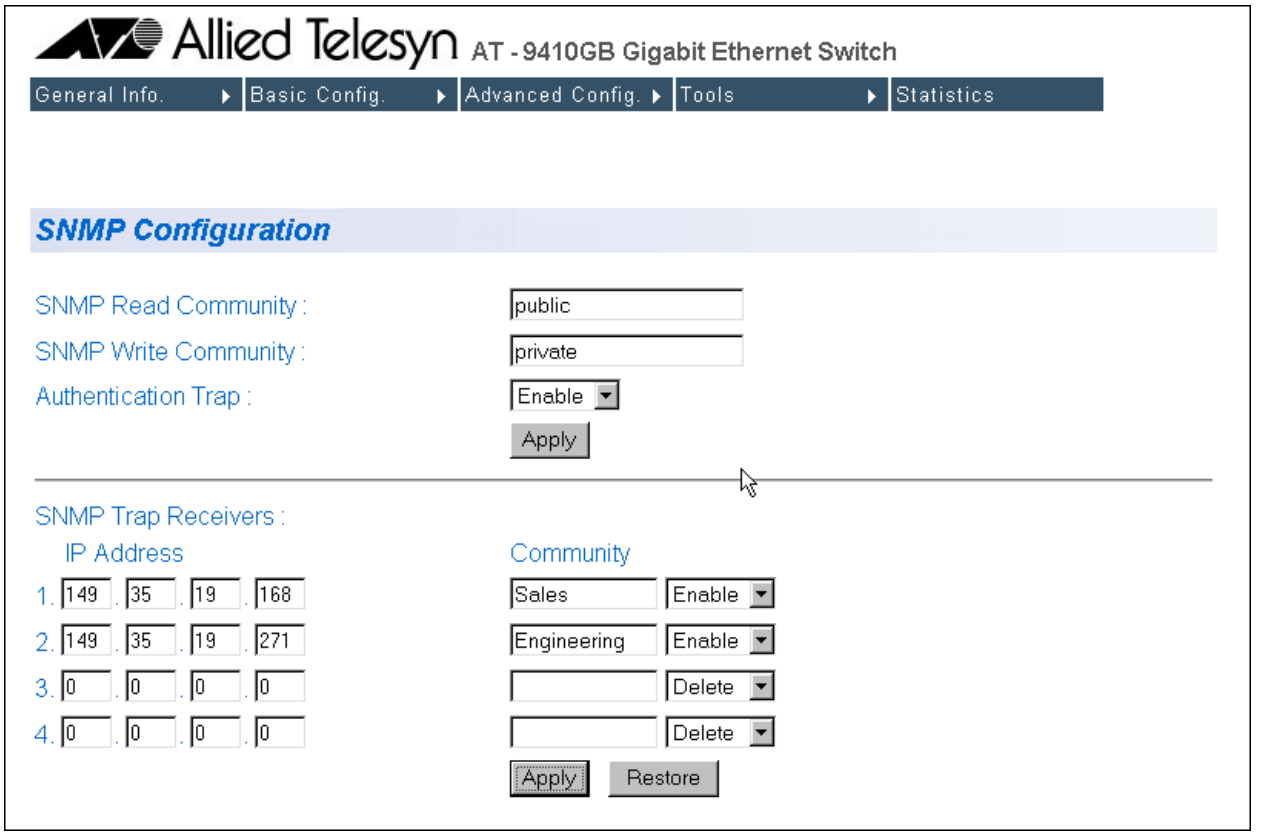

Figure 51 SNMP Configuration

2. Adjust the parameters as desired. The parameters are described below.

   Enable Community
   Disable Community
   Delete Community
   Use these parameters to set a switch's SNMP community strings.

   Trap Receiver 1
   Trap Receiver 2
   Trap Receiver 3

Trap Receiver 4
Use these selections to specify the IP addresses of up to four management workstations on your network to receive traps from the switch.

3. Click **Apply** to save your changes to the switch.
4. To restore the switch's default setting, click **Restore**.

   Changes are immediately activated on the switch.

Resetting a Switch

To reset a switch, perform the following procedure:

1. On the Home page, click on the **Tools** menu tab. The Tools sub-menu will appear. Choose **System Reboot** from the sub-menu.

   The System Reboot page in Figure 52 is displayed.

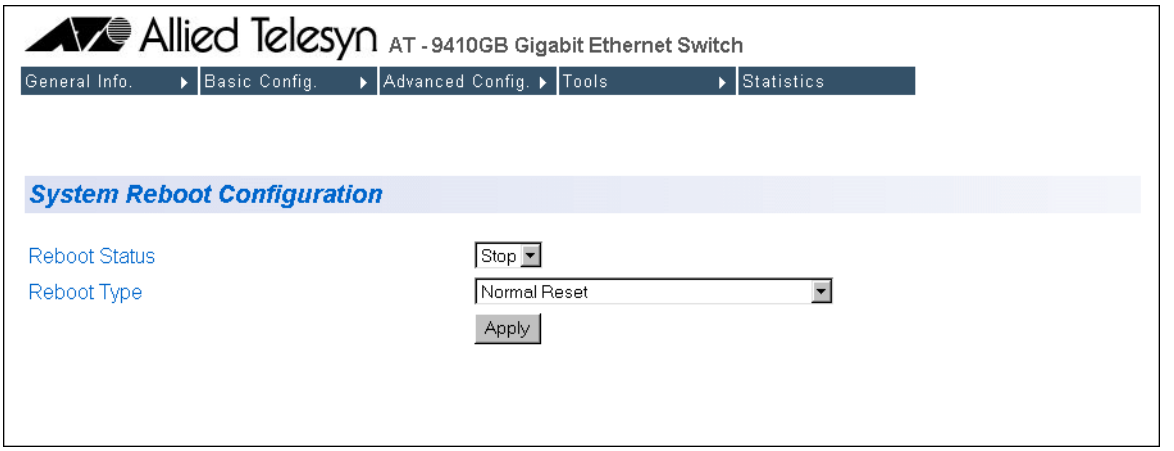

Figure 52 System Reboot

The options in the System Reboot page are defined below. Change the options as desired.

Reboot Status
Sets the reboot status of the switch. This parameter can be set to Start or Stop. The default setting is stop.

Reboot Type
Sets the reboot type of the switch. This parameter can be set to:

- **Factory Defaults**
  Resets the switch and returns all parameter settings to their factory default values.
- **Factory Defaults Except IP**
  Resets the switch and returns all parameter settings, except for the IP address, subnet mask, and gateway address, to their factory default values.
- **Normal Defaults**
  Resets the switch but retains all current parameter settings.

2. Select the desired reboot option from the Reboot Type field.
3. Select **Start** from the Reboot Status field.

4. Click **Apply**.

   This process takes approximately 1 minute to complete.

Caution
The switch will not forward traffic during the brief period required to reload its operating software. Some data traffic may be lost.

Viewing the AT-S45 Version Number and Switch MAC Address

To view basic information about the switch, perform the following procedure:

1. From the Home page, select **General Info.** and then select **Switch Info.** from the sub-menu.

   The Switch Information page in Figure 53 is displayed.

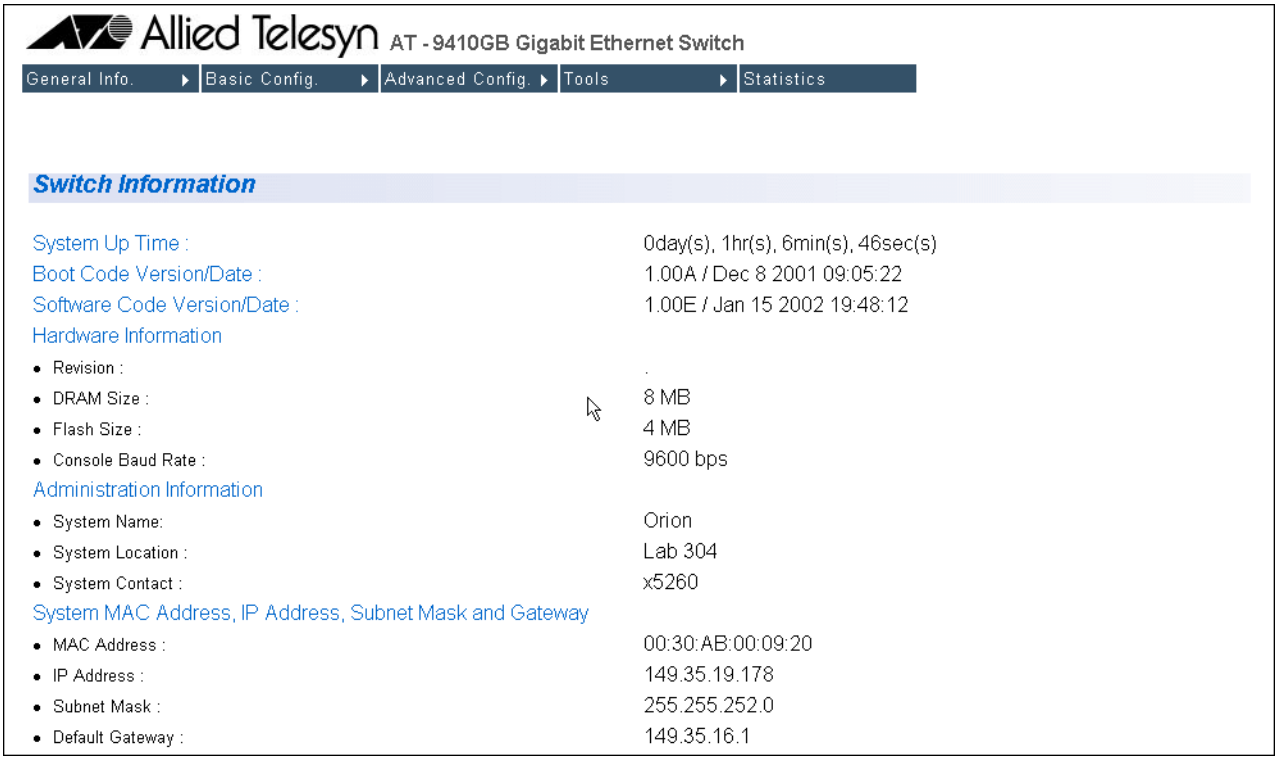
Allied Telesyn AT - 9410GB Gigabit Ethernet Switch
General Info.
Basic Config.
Advanced Config.
Tools
Statistics
Switch Information
System Up Time : 0day(s), 1hr(s), 6min(s), 46sec(s)
Boot Code Version/Date : 1.00A / Dec 8 2001 09:05:22
Software Code Version/Date : 1.00E / Jan 15 2002 19:48:12
Hardware Information
Revision :
DRAM Size : 8 MB
Flash Size : 4 MB
Console Baud Rate : 9600 bps
Administration Information
System Name: Orion
System Location : Lab 304
System Contact : x5260
System MAC Address, IP Address, Subnet Mask and Gateway
MAC Address : 00:30:AB:00:09:20
IP Address : 149.35.19.178
Subnet Mask : 255.255.252.0
Default Gateway : 149.35.16.1

Figure 53 Switch Information

This page is for viewing purposes only. You cannot change any of the values from this window. The sections in the window are defined below.

Hardware Information

This section displays the switch's current software version, DRAM size, flash size, and console baud rate.

Administration Information

This section displays the switch's name, location and contact information. These values are defined in the procedure **Configuring System Administration Information** on page 160, which also explains how to change the parameters.

System MAC Address, IP Address, Subnet Mask and Gateway
This section contains a variety of information, including the IP address of the switch and the system name. These parameters are defined in the procedure **Configuring an IP Address** on page 158, which also explains how to change the parameters.

Pinging a Network Device

To configure the ping execution settings on the switch, perform the following procedure:

1. Click on the **Tools** menu tab and select **Ping** from the sub-menu.

   The Ping Test Configuration page is displayed, as shown in Figure 54.

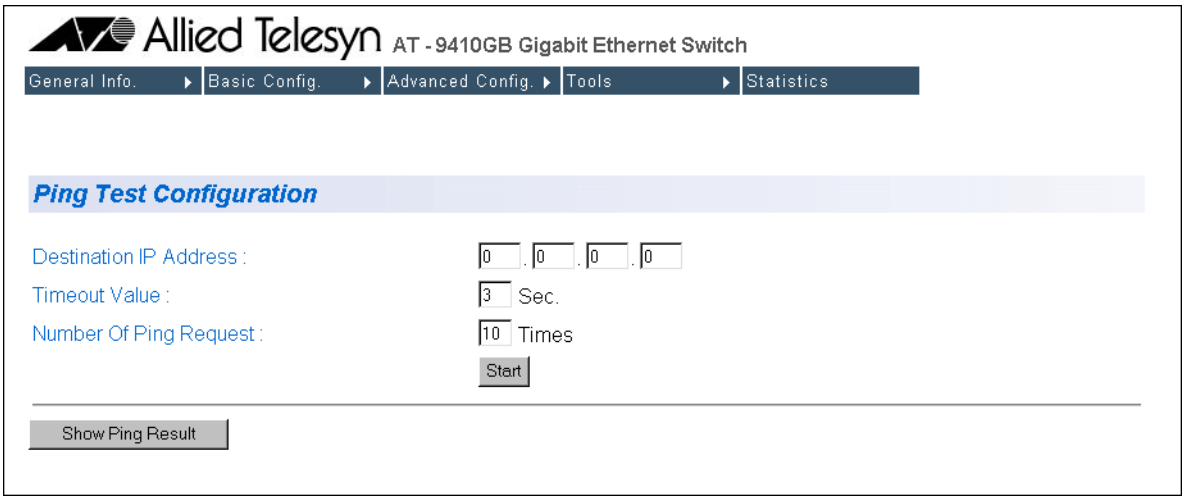

Figure 54 Ping Test Configuration

2. Adjust the parameters as desired. To change a value, enter the new information in the data entry field. The parameters are described below.

   Destination IP Address
   This command specifies the IP address of the end node you are pinging.

   Timeout Value
   The length of time for which the switch will continue to send pings if it does not receive a response. The default timeout setting is 3 seconds.

   Number of Ping Requests
   Number of ping attempts the switch should make before it stops pinging if it does not receive a response. The default number of ping requests is 10.

3. Click the Start button.

4. To view the ping results, click the Show Ping Results button.

The Ping Test Result page is displayed, as shown in Figure 55.

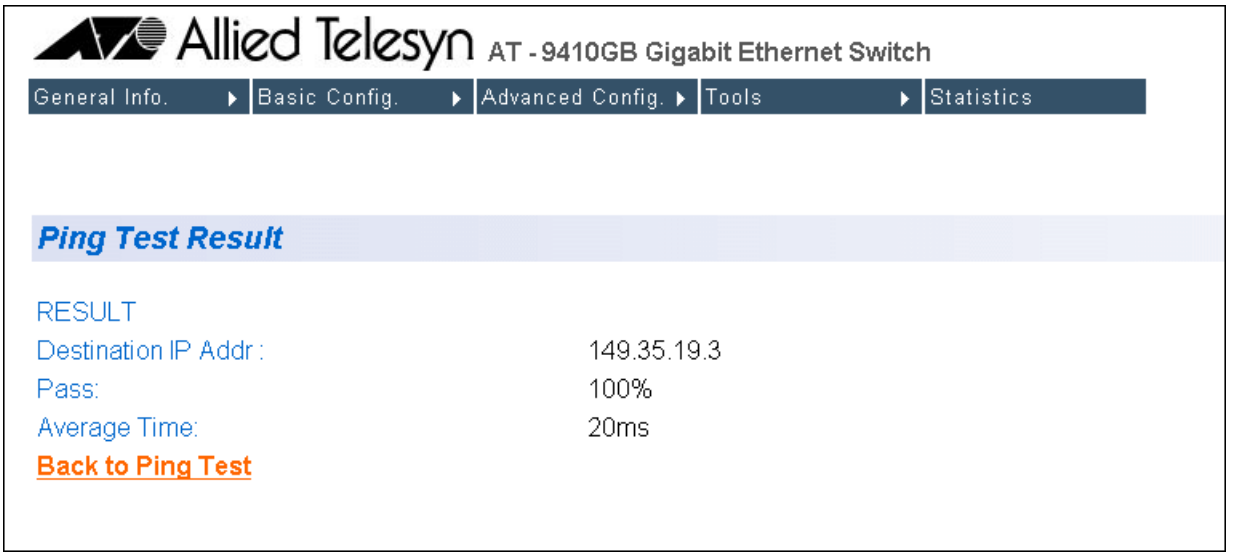

Figure 55 Ping Test Result

The parameters cannot be modified on this page. They are for informational purposes only. The parameters are described below.

Destination IP Address
This is the IP address you entered on the Ping Test Configuration page.

Pass
Number of successful pings.

Average Time
Average length of time for each ping request.

5. Use the Back to Ping Test link to return to the Ping Test Configuration page.

Bootstrap Configuration

The bootstrap feature allows you to download new software and configuration settings when you boot up the switch.

To configure the bootstrap settings on the switch, perform the following procedure:

1. Click on the **Tools** menu tab and select **Bootstrap** from the sub-menu.

   The Bootstrap Configuration page is displayed, as shown in Figure 56.

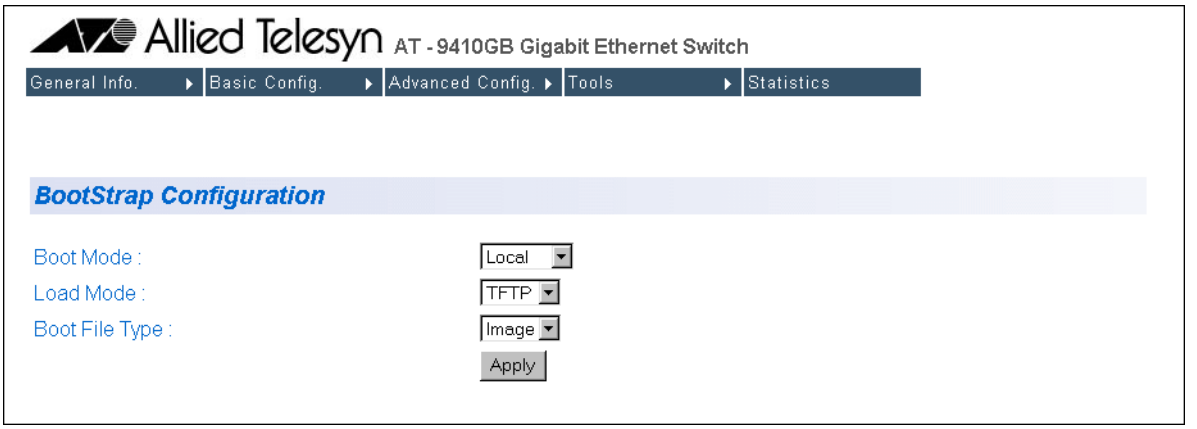

Figure 56 Bootstrap Configuration

2. Adjust the parameters as desired. To change a parameter setting, select the option from the pull-down menu and click the Apply button. The parameters are described below.

   Boot Mode
   Allows the user to determine how the switch should boot up. There are two boot load options: local and remote.

   - **Local**
     If you choose the local boot load mode, the switch boots using the management software that is saved in the switch memory. This is the default boot load mode. If you are going to use the local boot load mode, you do not need to configure any of the other parameters on the Bootstrap Configuration Menu and the switch will not download any files when it boots up.

   - **Remote**
     If you choose the remote boot load mode, the switch downloads software from a TFTP server and boots using the newly downloaded management software.

Load Mode
If you are using the remote boot load mode, you need to specify how the switch should download the new management software. There are two boot mode options: DHCP and TFTP.

- **DHCP**
  If you choose the DHCP boot mode, the switch will use DHCP to determine the switch IP address, the TFTP server address, and the image or configuration file name. The switch will use this information to download the management software from the TFTP server.

- **TFTP**
  If you choose the TFTP boot mode, the switch will use the IP address that you assigned to the switch on the System IP Configuration Menu as well as the TFTP server address and the image or configuration file name that you entered in the TFTP section of the Software Upgrade Menu.

Boot File Type
If you selected the remote boot load mode, you can choose what kind of files the switch will download while it is booting up. There are three file type options:

- **Image**
  An image file is the management software for the switch.

- **Configuration**
  A configuration file is a file that contains all of the existing configurations and settings for a switch. You can upload the configuration file and modify the switch settings and then download the configuration file back to the switch or onto multiple switches that you want to have the same configurations. The switch(es) will then update their configuration(s) based on the settings in the configuration file.

- **Image and Configuration**
  This option allows you to download both the management software and the configuration file.

Chapter 18
Port Parameters

The procedures in this chapter allow you to view and change the parameter settings for the individual ports on a switch. Examples of port parameters that you can adjust include duplex mode and port speed.

This chapter contains the following procedures:

- ❑ **Configuring Port Parameters** on page 177
- ❑ **Displaying Port Status** on page 179
- ❑ **Displaying Statistics** on page 182

Configuring Port Parameters

To configure the parameter settings for a port on a switch, perform the following procedure:

1. From the Home page, select **Basic Config.** and then select **Port Config.** from the sub-menu.

   The Port Configuration window is shown in Figure 57.

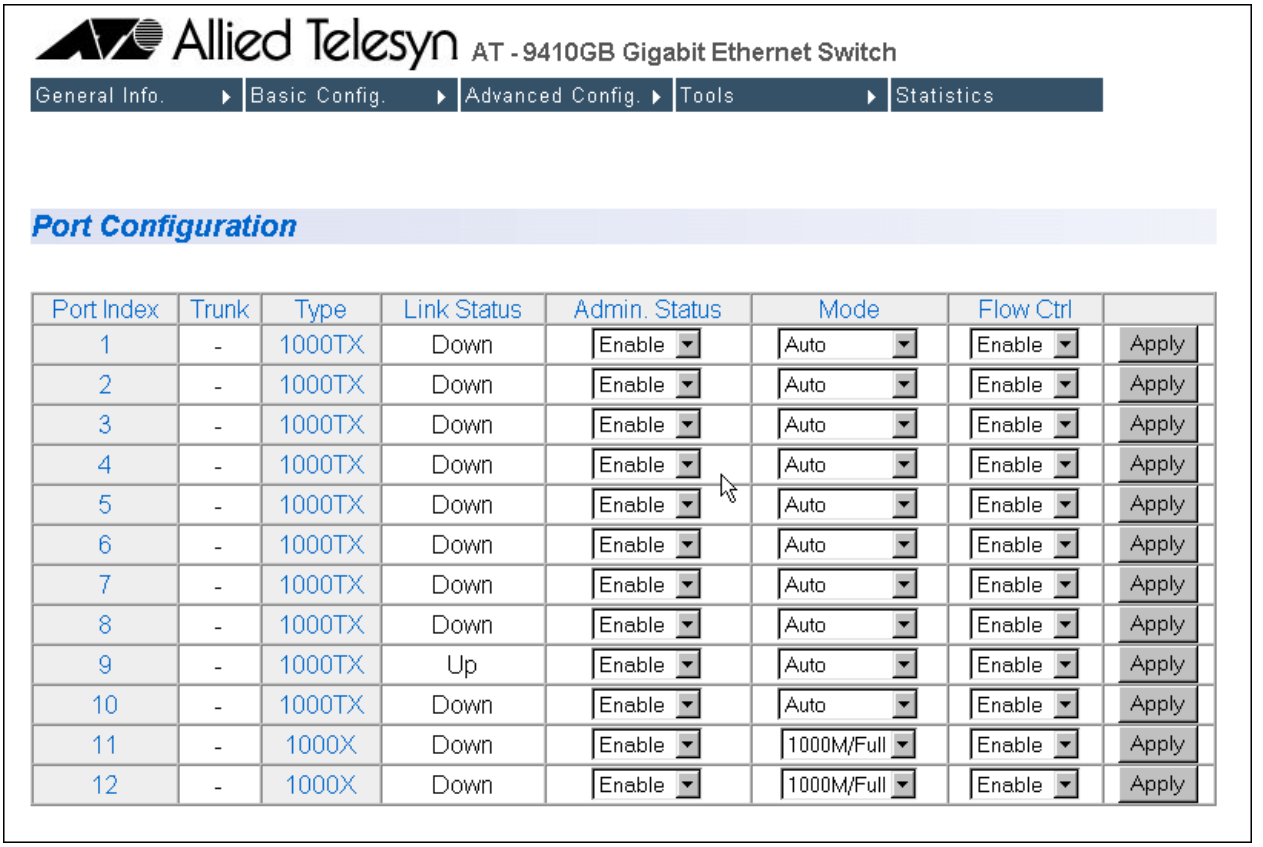
Allied Telesyn AT - 9410GB Gigabit Ethernet Switch
General Info.
Basic Config.
Advanced Config.
Tools
Statistics
Port Configuration
Port Index | Trunk | Type | Link Status | Admin. Status | Mode | Flow Ctrl
1 - 1000TX Down Enable Auto Enable Apply
2 - 1000TX Down Enable Auto Enable Apply
3 - 1000TX Down Enable Auto Enable Apply
4 - 1000TX Down Enable Auto Enable Apply
5 - 1000TX Down Enable Auto Enable Apply
6 - 1000TX Down Enable Auto Enable Apply
7 - 1000TX Down Enable Auto Enable Apply
8 - 1000TX Down Enable Auto Enable Apply
9 - 1000TX Up Enable Auto Enable Apply
10 - 1000TX Down Enable Auto Enable Apply
11 - 1000X Down Enable 1000M/Full Enable Apply
12 - 1000X Down Enable 1000M/Full Enable Apply

Figure 57 Port Configuration window

2. Adjust the port parameter(s) that you want to configure. You can configure only one port at a time.

   The parameters are described below.

   Port Index
   This number specifies the number of the port of the switch. This parameter can not be changed.

   Trunk
   This number specifies the number of the trunk that the port resides in, if any. For instructions on how to create a port trunk, refer to **Port Trunks** on page 189.

Type
This number specifies the maximum operating speed of the port.

Link Status
The link status between the port and the end node connected to the port. Possible values are:

Up - indicates that a valid link exists between the port and the end node.

Down - indicates that the port and the end node have not established a valid link.

Admin. Status
The current operating status on the port. Possible values are:

Enabled - Indicates that the port is enabled.

Disabled - Indicates that the port is disabled.

Mode
The operating speed and duplex mode of the port. Possible settings for this parameter are:

- ❑ Auto-Negotiate: The port will Auto-Negotiate both speed and duplex mode. This is the default.
- ❑ 1000Mbps - Half Duplex
- ❑ 100Mbps - Full Duplex
- ❑ 10Mbps - Full Duplex
- ❑ 1000Mbps - Half Duplex
- ❑ 100Mbps - Half Duplex
- ❑ 10Mbps - Half Duplex

Flow Control
The flow control setting for the port. Possible values are:

Enabled - Flow control is activated on the port.

Disable - No flow control on the port.

3. Once you have made the desired changes, click **Apply**.

   The switch immediately activates the parameter changes on the port.

Displaying Port Status

The procedure in this section displays the operating status of the ports on a switch. To display the status of a switch port, perform the following procedure:

1. From the Home page, select **General Info.** and then select **Front Panel** from the sub-menu.

   The Front Panel window is shown in Figure 58.

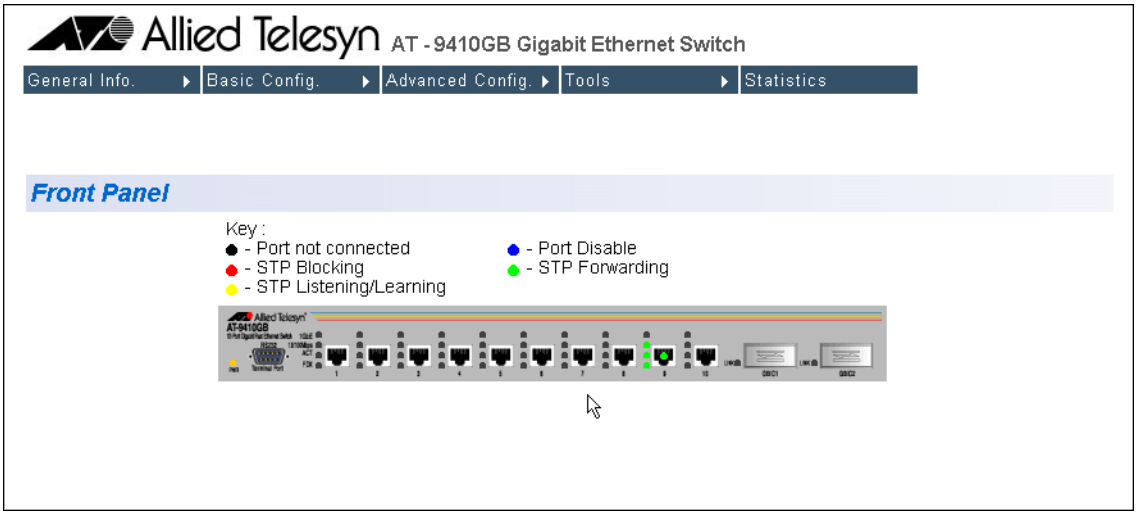

Figure 58 Front Panel window

   This page displays a graphical image of the front of the switch. Ports with valid links to end nodes have a green light.

2. Click a port. You can select only one port at a time.

The Configuration of a Port window in Figure 59 is displayed.

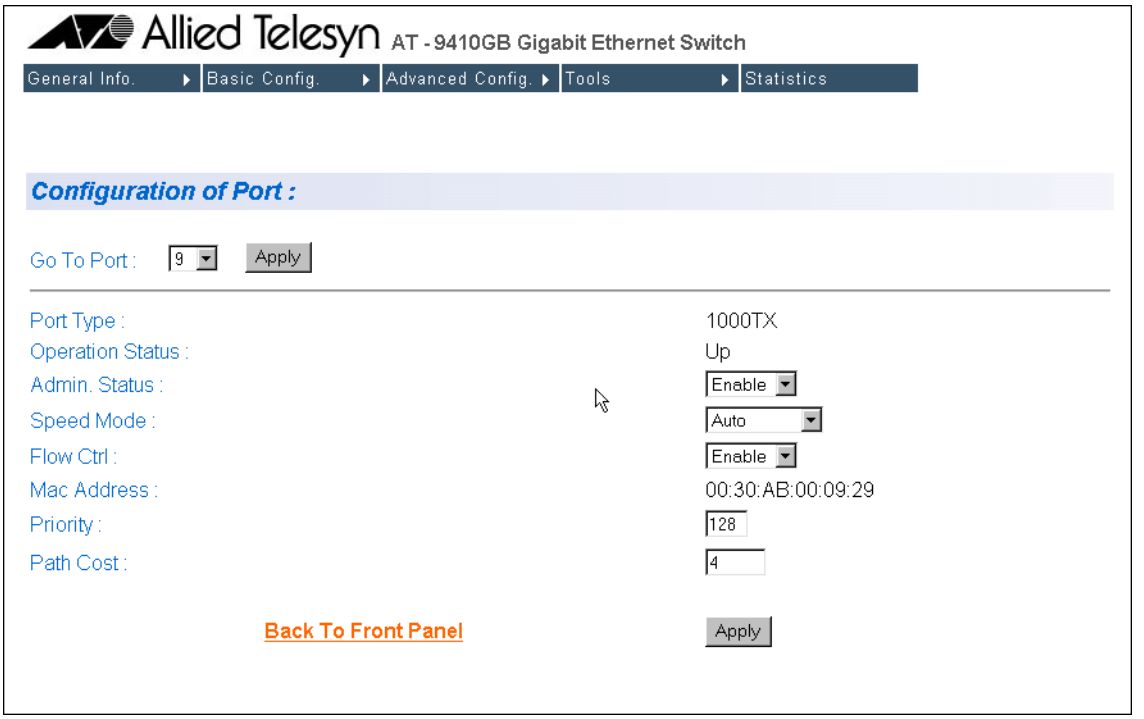

Figure 59 Configuration of a Port Window

This window displays the port's configuration and operating status.

Set the port parameters as desired. You can set a parameter by clicking in field you desire to modify. The parameters are described below.

Port Type
This number specifies the maximum operating speed of the port. This parameter can not be changed.

Operation Status
The status of the link between the port and the end node connected to the port. Possible values are:

Up - indicates that a valid link exists between the port and the end node.

Down - indicates that the port and the end node have not established a valid link.

Admin. Status
The current operating status on the port. Possible values are:

Enabled - Indicates that the port is enabled.

Disabled - Indicates that the port is disabled.

Speed Mode
The operating speed and duplex mode of the port. Possible settings for this parameter are:

- ❑ Auto-Negotiate: The port will Auto-Negotiate both speed and duplex mode. This is the default.
- ❑ 1000Mbps - Half Duplex
- ❑ 100Mbps - Full Duplex
- ❑ 10Mbps - Full Duplex
- ❑ 1000Mbps - Half Duplex
- ❑ 100Mbps - Half Duplex
- ❑ 10Mbps - Half Duplex

Flow Control
The port's flow control setting. Possible values are:

Enable - Flow control is activated on the port.

Disable - No flow control on the port.

MAC Address
This specifies the MAC address of the port.

Priority
This parameter applies only when the switch is using STP. The parameter is used as a tie breaker when two or more ports have equal costs to the root bridge. The range is 0 - 255.

Path Cost
This parameter applies only when the switch is using STP. This parameter is used in deciding which port has the lowest cost to the root bridge.

Displaying Statistics

The procedure in this section displays the statistics of a port on a switch. To display the statistics of a port, perform the following procedure:

1. From the Home page, select **Statistics** from the menu.

   The Statistics window is shown in Figure 60.

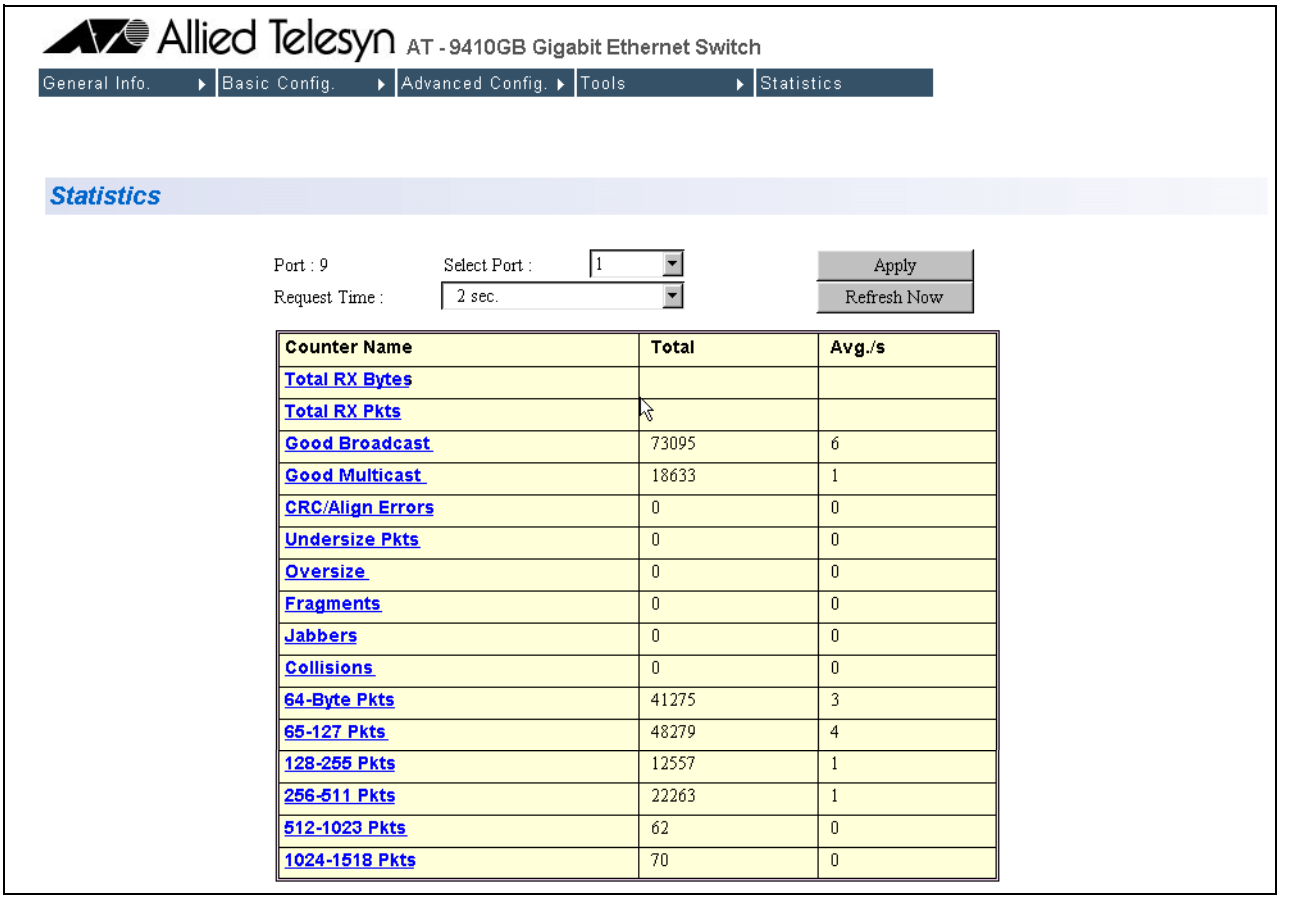

Figure 60 Statistics Window

2. To view statistics on a port, click and select a port on the **Select Port** parameter.
3. Click **Apply**.

   The information in this window is for viewing purposes only. The statistics are defined below:

   Total RX Bytes
   Number of bytes received on the port.

   Total RX Packets
   Number of packets received on the port.

Good Broadcast
Number of valid broadcast packets received on the port.

Good Multicast
Number of valid multicast packets received on the port.

CRC/Align Errors
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Undersize Packets
Number of packets that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Oversize Packets
Number of packets exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Fragments
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.

Jabbers
Number of electrical signal errors detected on the port.

Collisions
Number of packet collisions on the port.

64-Byte Pkts
Number of 64-byte packets sent or received by the port. The minimum length of an Ethernet packet is 64 bytes.

65-127 Pkts
Number of 65- to 127-byte packets sent or received by the port.

128-255 Pkts
Number of 128- to 255-byte packets sent or received by the port.

256-511 Pkts
Number of 256- to 511-byte packets sent or received by the port.

512-1023 Pkts
Number of 512- to 1023-byte packets sent or received by the port.

1023-1518 Pkts
Number of 1023- to 1518-byte packets sent or received by the port. The maximum length of an Ethernet packet is 1518 bytes.)

Chapter 19
Port Security

This chapter contains the procedures for setting port security. The sections in this chapter include:

- ❑ **Configuring Port Security** on page 186
- ❑ **Displaying Port Security Settings** on page 188

Note
For background information on port security, refer to **Port Security Overview** on page 58.

Configuring Port Security

To configure the switch's port security, perform the following procedure:

1. From the Home page, select the **Advanced Config** menu tab and then select the **Port Security** tab in the sub-menu. Select **Security Config** from the next sub-menu.

   The Port Security window in Figure 61 as displayed.

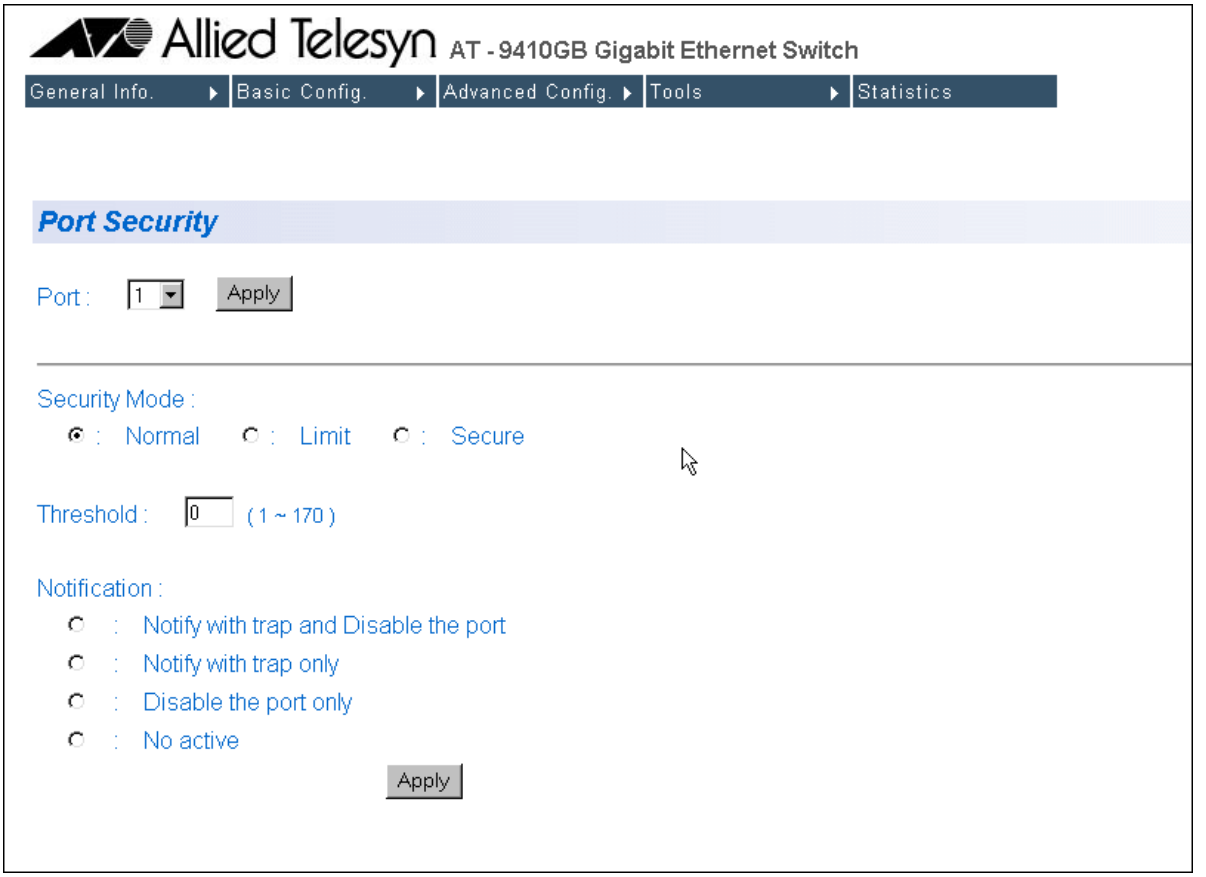

Figure 61 Port Security Window

2. Select the port whose security you would like to configure from the Port pull-down menu.
3. Select a security level for the port by checking one of the radio buttons below Security Mode: The options are Normal, Limit, and Secure. For a description of these security levels, refer to **Port Security Overview** on page 58.

Note
The default Security Mode is Normal.

4. If you selected the Limit security level, set a threshold for the maximum number of dynamic MAC addresses the port can learn. The default threshold is 1. Enter the number of dynamic MAC addresses (between 1 and 170) in the threshold field you want the port to be able to learn.

   Note
   A threshold cannot be set for the port if the security level is set to Normal or Secure.

5. To control what happens on the port once the threshold has been met, check one of the radio buttons next to the intrusion detection Notification options.

   The options are:

   - ❑ No action
   - ❑ Disable the port only
   - ❑ Notify with trap only
   - ❑ Notify with trap and disable the port

6. To configure the security for another port, select the port number from the Port pull-down menu at the top of the Port Security page and repeat this process.
7. To verify the new port security configurations and to see the security settings for all of the ports at once, continue to the next section, **Displaying Port Security Settings** on page 188.

Displaying Port Security Settings

To view the switch's port security settings, perform the following procedure:

1. On the Home page, select the **Advanced Config** menu tab and then select **Port Security** from the sub-menu. Select **Security Overview** from the next sub-menu.

   The Port Security Overview page will appear, as displayed in Figure 62, allowing you to see the security settings for all of the ports on a switch.

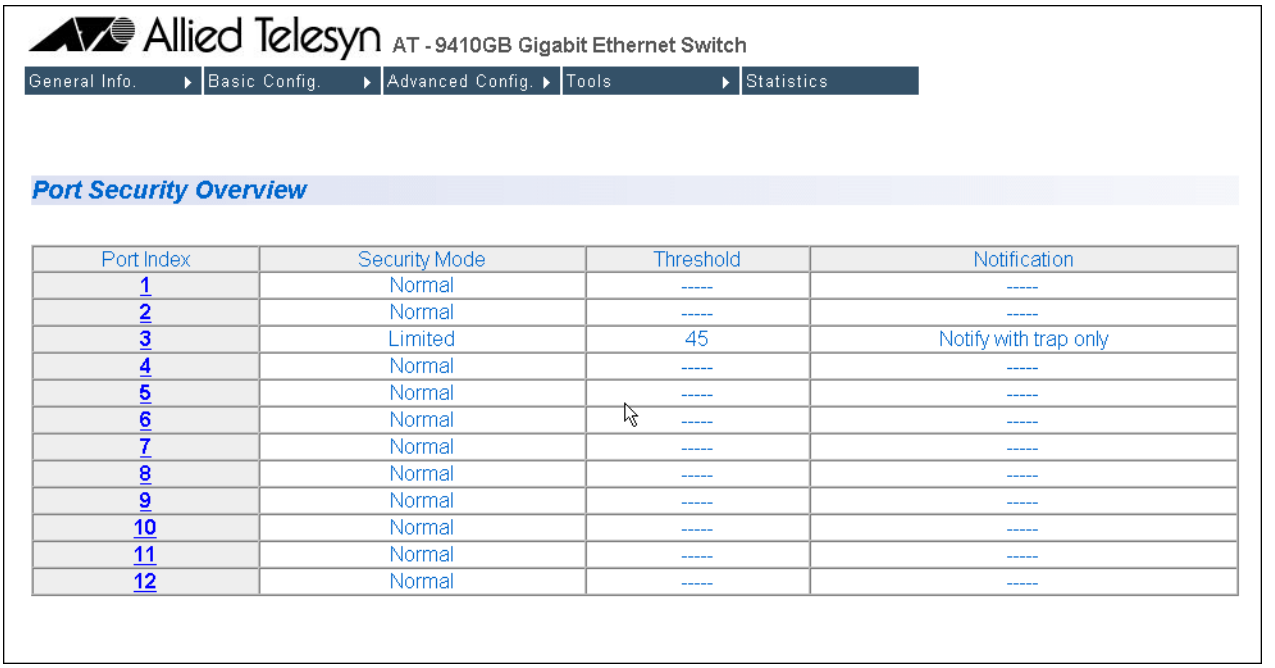

Figure 62 Port Security Overview Window

2. To change the security settings for a port, click on the port number in the Port Index column on the left-hand side of the page. You will be taken to the Port Security page, where you can configure port security as described in the previous section.

Chapter 20
Port Trunks

This chapter contains the procedure for creating or deleting a port trunk from a web browser management session.

- ❑ **Creating or Deleting a Port Trunk** on page 190

Note
For background information on port trunking, refer to **Port Trunking Overview** on page 64.

Creating or Deleting a Port Trunk

Caution

Do not connect the cables of a port trunk to the ports on the switch until after you have configured the ports on both the switch and the end node. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms, which can adversely effect the operations of your network.

If you are deleting a port trunk, disconnect the cables from the ports before you delete the trunk. Deleting the trunk without first disconnecting the data cables can create a loop in your network topology, which can produce broadcast storms.

To create or delete a port trunk, perform the following procedure:

1. From the Home page, select **Advanced Config.** and then select **Trunk Config.** from the sub-menu.

   The management software displays the Trunk Configuration window in Figure 63.

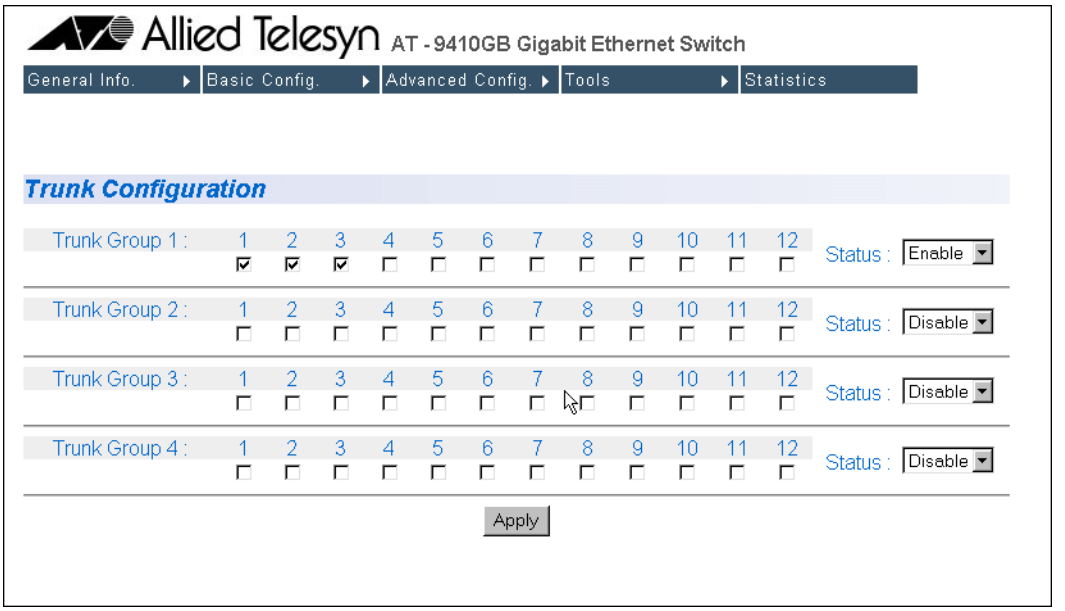
Allied Telesyn AT - 9410GB Gigabit Ethernet Switch
General Info.
Basic Config.
Advanced Config.
Tools
Statistics
Trunk Configuration
Trunk Group 1 : 1 2 3 4 5 6 7 8 9 10 11 12 Status : Enable
Trunk Group 2 : 1 2 3 4 5 6 7 8 9 10 11 12 Status : Disable
Trunk Group 3 : 1 2 3 4 5 6 7 8 9 10 11 12 Status : Disable
Trunk Group 4 : 1 2 3 4 5 6 7 8 9 10 11 12 Status : Disable
Apply

Figure 63 Trunk Configuration Window

   If the switch does not contain a port trunk, all ports in the switch image will not be checked. If there is a port trunk, the ports of the trunk will be checked.

2. To create a port trunk, do the following:

a. Click the ports that will make up the port trunk. A port trunk can contain 2, 3, or 4 ports.

b. Click on the Status field, select **Enable**.

The new port trunk is immediately activated on the switch. You can now connect the data cables to the ports of the trunk on the switch.

3. To delete a port trunk, deselect all port members of the trunk you want to delete.
4. Click on the Status field and select **Disable**.
5. Click **Apply**.

Chapter 21
Port Monitoring

This chapter contains the procedure for creating or deleting a port monitor.

- ❑ **Creating or Deleting a Port Monitor** on page 193

Note
For background information on port monitoring, refer to **Port Monitoring Overview** on page 72.

Creating or Deleting a Port Monitor

To create or delete a port monitor, perform the following procedure:

1. From the Home page, select **Advanced Config.** and then select **Port Monitoring** from the sub-menu.

   The management software displays the Port Monitoring Configuration window in Figure 64.

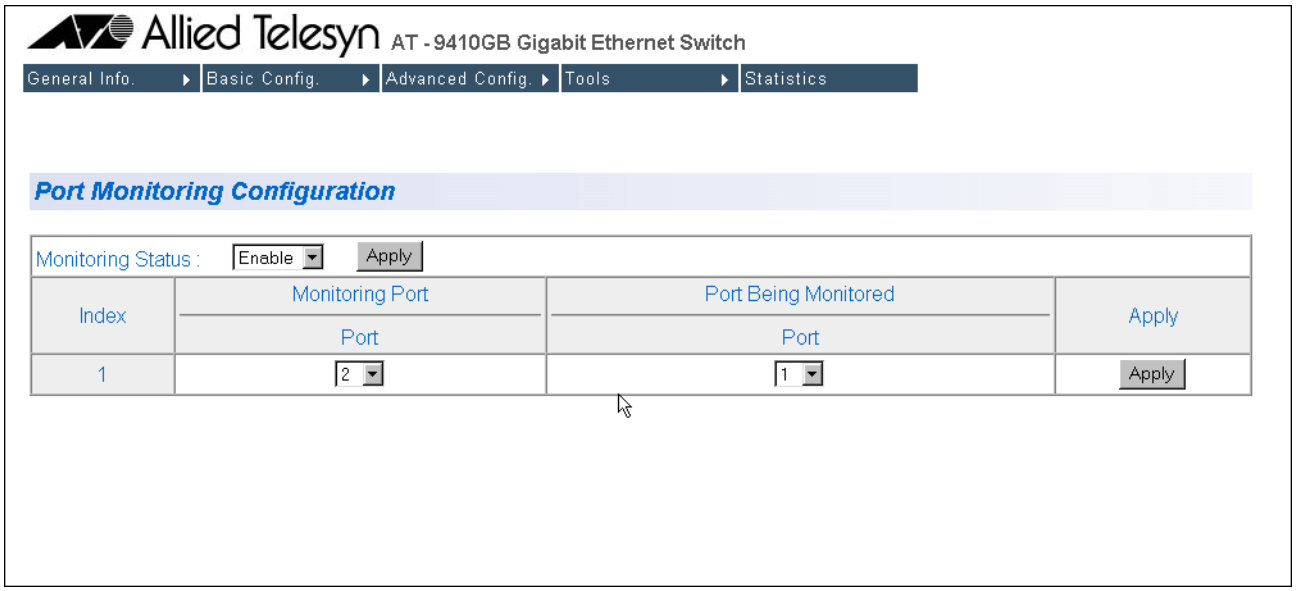

Figure 64 Port Monitoring Configuration Window

2. To create a port monitor, do the following:

   a. Use the pull-down menu from Monitoring Port to select the port to function as the port monitor.

   b. Use the pull-down menu from Port Being Monitored to select the port whose traffic is to be copied to the monitor port. You can select from 1 to 12 ports.

   c. Click **Apply**.

   d. Select the Monitoring Status pull-down menu, click **Enable**.

   e. Click **Apply**.

   The port monitor is immediately activated on the switch. You can now connect a data analyzer to the monitor port to monitor the traffic on the selected port.

3. To delete an existing port monitor, select **Disable** from the Monitoring Status pull-down menu and click **Apply**.

   The port monitor is deleted. The port that was functioning as the monitor port can now be used for normal network operations.

Chapter 22
Spanning Tree Protocol

This chapter explains how to configure the STP bridge parameters on an AT-9410GB Gigabit Ethernet Switch from a web browser management session.

Sections in the chapter include:

- **Configuring a Bridge's STP Settings** on page 196
- **Configuring STP Port Settings** on page 198

Note
For background information on STP, refer to **STP Overview** on page 77.

Configuring a Bridge's STP Settings

> **Caution**
> STP on a bridge is disabled by default. If you enable STP, the bridge provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

To configure a bridge's STP parameters, perform the following procedure:

1. From the Home page, click on **Basic Config.**, **Spanning Tree** and then **STP Config.** from the sub-menu.

   The Spanning Tree Bridge Configuration window in Figure 65 is displayed.

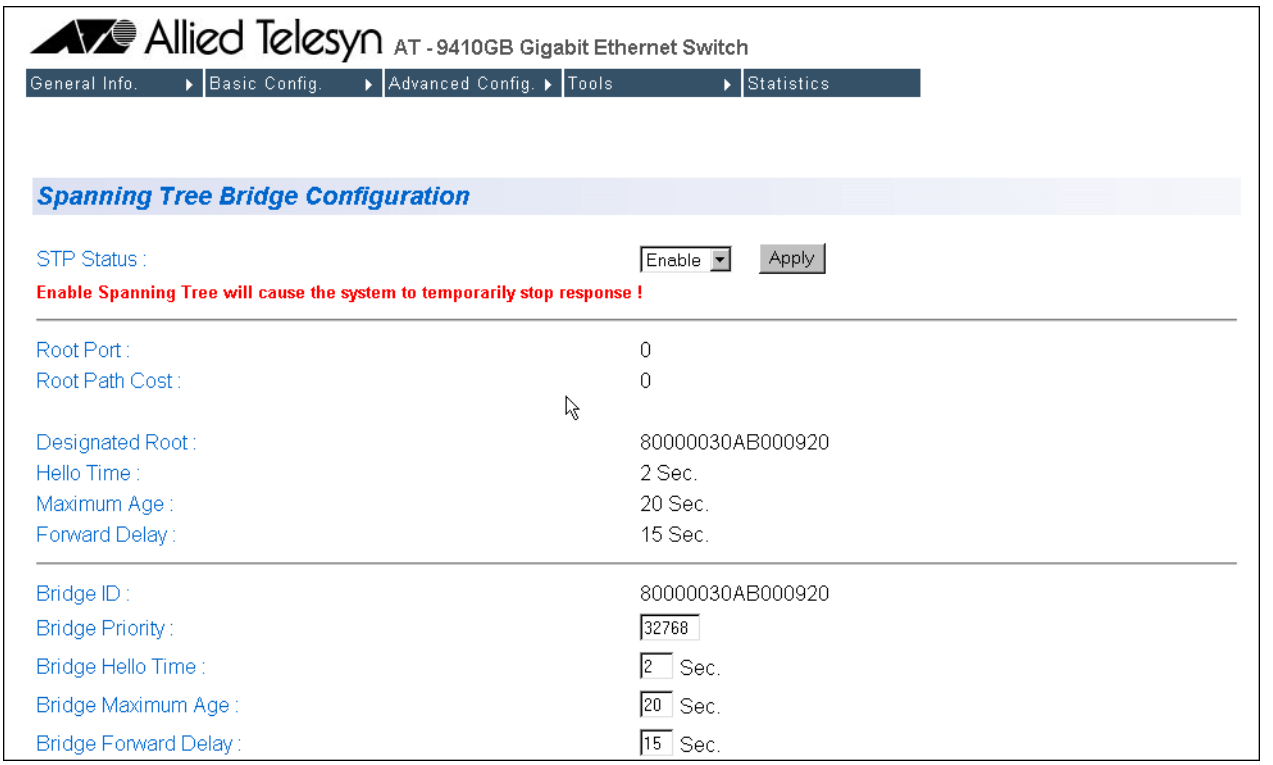
Allied Telesyn AT - 9410GB Gigabit Ethernet Switch
General Info.
Basic Config.
Advanced Config.
Tools
Statistics
Spanning Tree Bridge Configuration
STP Status :
Enable
Apply
Enable Spanning Tree will cause the system to temporarily stop response !
Root Port : 0
Root Path Cost : 0
Designated Root : 80000030AB000920
Hello Time : 2 Sec.
Maximum Age : 20 Sec.
Forward Delay : 15 Sec.
Bridge ID : 80000030AB000920
Bridge Priority : 32768
Bridge Hello Time : 2 Sec.
Bridge Maximum Age : 20 Sec.
Bridge Forward Delay : 15 Sec.

Figure 65 Spanning Tree Window - Configuration

2. Adjust the bridge STP settings as needed. The parameters are described below.

Enable/Disable STP
Enables and disables STP on the switch. The default setting is disabled.

Bridge Priority
The priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 65,535, with 0 being the highest priority.

Bridge Hello Time
The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Bridge Maximum Age
The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

Note
The aging time for BPDUs is different from the aging time used by the MAC address table.

Bridge Forward Delay
The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The default is 15 seconds.

3. After you have made the desired changes, click **Apply**.

   Changes are immediately activated on the switch.

Configuring STP Port Settings

To display and configure the STP port settings, perform the following procedure:

1. From the Home page, click on **Basic Config.**, **Spanning Tree** and then **STP Port Config.** from the sub-menu.

   The Spanning Tree Port Configuration window in Figure 66 is displayed.

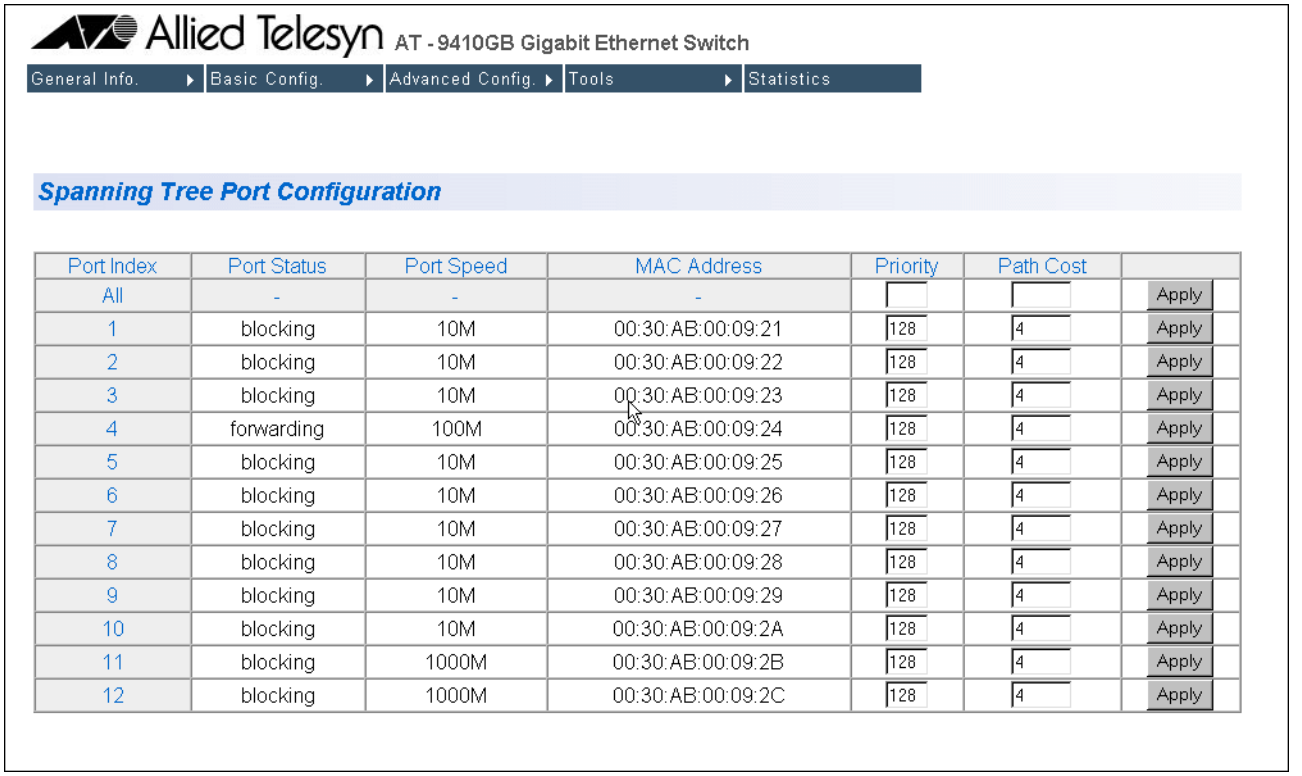

Figure 66 Spanning Tree Port Configuration

2. Adjust the parameter settings as desired. The parameters are described below.

   The 9410GB Gigabit Ethernet Switch has the "All" setting that allows a global setting to be set for all ports on the switch.

3. Click **Apply**.

Priority
This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0-255. The default value for priority is 128.

Note
Port Priority can not be set on ports that are part of a trunk group.

Path Cost
The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The default values for this parameter are 100 for a 10 Mbps port, 10 for a 100 Mbps port, and 4 for a 1 Gbps port. The range is 1 to 65535.

This following information is for display purposes only and cannot be changed from the Spanning Tree Port Configuration Menu.

Port Index
The port number on the switch. "All" indicates a setting that includes all ports on the switch.

Port Status
The current STP status of the port. Possible values are:

- ❑ Forwarding
- ❑ Listening
- ❑ Learning
- ❑ Blocking

Port Speed
The current operating speed of the port.

MAC Address
The MAC address of the port.

Chapter 23
Virtual LANs

This chapter explains how to create, modify, and delete VLANs from a web management session.

> **Note**
> For background information on VLANs, refer to **Chapter 9, Virtual LANs**.

This chapter contains the following sections:

- ❑ **Creating a Tagged or Untagged VLAN** on page 202
- ❑ **Viewing or Modifying a Tagged or Untagged VLAN** on page 206
- ❑ **Deleting a Tagged or Untagged VLAN** on page 211
- ❑ **Creating a Port-based VLAN** on page 212
- ❑ **Viewing or Modifying a Port-based VLAN** on page 214
- ❑ **Setting GVRP Status** on page 216
- ❑ **Resetting the VLAN Parameters to Default** on page 217
- ❑ **Setting the VLAN Type** on page 218

Creating a Tagged or Untagged VLAN

The procedure for creating a new VLAN is divided into the following phases:

- ❑ Phase 1: Assigning a VID and name and specifying the port members
- ❑ Phase 2: Converting tagged ports into untagged ports

Performing Phase 1 is required whenever you create a new VLAN. Every VLAN must have a name, VID, and, of course, ports. You will need to perform Phase 2 if some or all of the ports of a VLAN will be untagged ports. Ports that you want to function as untagged ports must be converted by changing their PVIDs, as explained in Phase 2.

To create a new VLAN, start by performing the procedure in Phase 1.

Phase 1

This phase assigns a VID and a name to your VLAN, and also designates the VLAN port members.

1. On the Home page, select the **Advanced Config** menu tab and then select **VLAN Config** from the sub-menu. Select **Create VLAN** from the sub-menu.

   The Create/Modify VLAN page will appear, as displayed in Figure 67

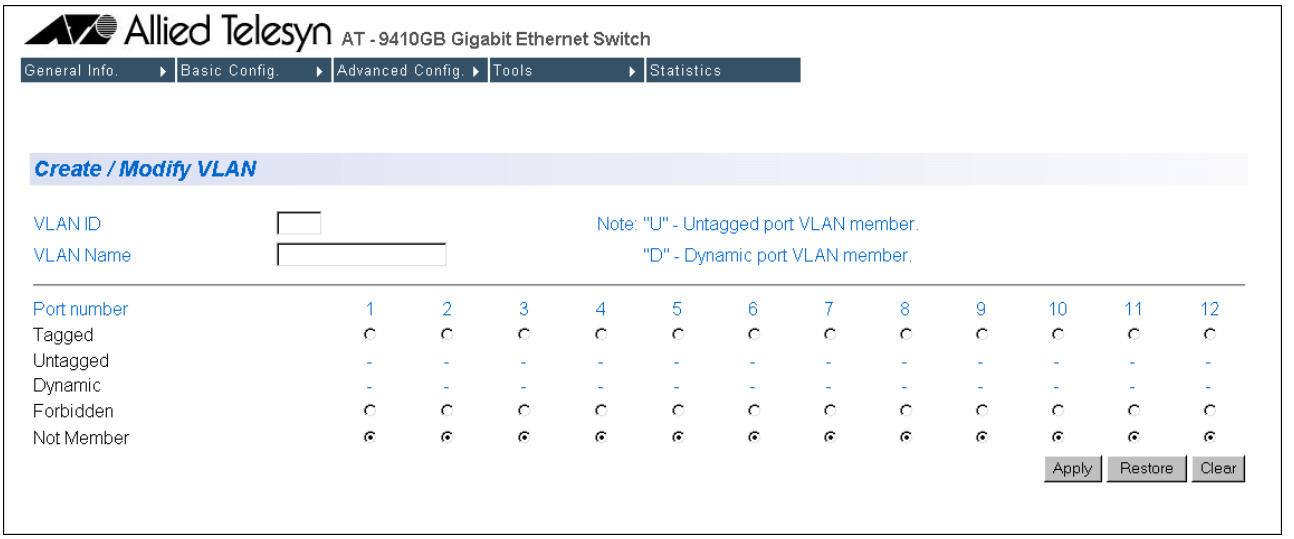

Figure 67 Create/Modify VLAN

Note
Check the VLAN Type field in the window to make sure it is set to 802.1Q, which happens to be the default. You can create tagged and untagged VLANs only when the switch is operating in the 802.1Q mode. For instructions on how to change the switch's VLAN mode, refer to **Setting the VLAN Type** on page 218.

2. Enter a VLAN ID in the VLAN ID field.

   If this VLAN will be unique in your network, then its VID must also be unique from all other VIDs in the network.

   If this VLAN will be part of a larger VLAN that spans multiple switches, than the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that will span three switches, you must assign the Sales VLAN on each of the switches the same VID value.

   The VLAN ID must be a value between 2 and 4094.

3. Enter a name for the VLAN of up to 32 characters in the VLAN Name field.

   The name should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name spaces, but not special characters, such as asterisks (*) or exclamation points (!).

   If the VLAN will be unique in your network, then the name should be unique as well.

   If the VLAN will be part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

4. In the Tagged row in the window, select the radio buttons for *both* the tagged and untagged ports that are to be members of the new VLAN.

   Note
   The procedure in Phase 2 explains how to convert tagged ports into untagged ports by changing the PVIDs.

   Note
   The rows Forbidden and Not Member are explained in the section **Setting GVRP Status** on page 216.

5. Click the **Apply** button at the bottom right-hand side of the window.

   You have now created a new VLAN. You gave it a VID and a name. You also specified which ports were to be members of the new VLAN.

However, it is important to note that, by default, all of the ports that you just added to the new VLAN are tagged ports, meaning they are shared ports. The ports are still members of their current VLANs.

If you want to convert the ports into untagged ports, you must perform the procedure in Phase 2.

Note
There are two additional buttons in the bottom right-hand corner of the page. The Restore button will cancel any changes you have made to the VLAN since using the Apply button. The Clear button removes all checks from all radio buttons, letting you select each port's configuration. If you leave any port columns blank when you click the Apply button, the management software will assign those ports to the Not Member row.

Phase 2 This phase to creating a new VLAN converts the tagged ports that you added to the new VLAN into untagged ports. This involves changing the PVIDs of the ports so that they match the VID of the new VLAN. For example, if you assigned the new VLAN a VID of 4, you must change the PVIDs of the untagged ports to 4. The following procedure explains how this is accomplished.

The following procedure assumes that you are continuing directly from Phase 1.

1. On the Home page, select the **Advanced Config** menu tab and then select **VLAN Config** from the sub-menu. Select **VLAN Port Config** from the next sub-menu.

The VLAN Port Config page will appear, as displayed in Figure 68

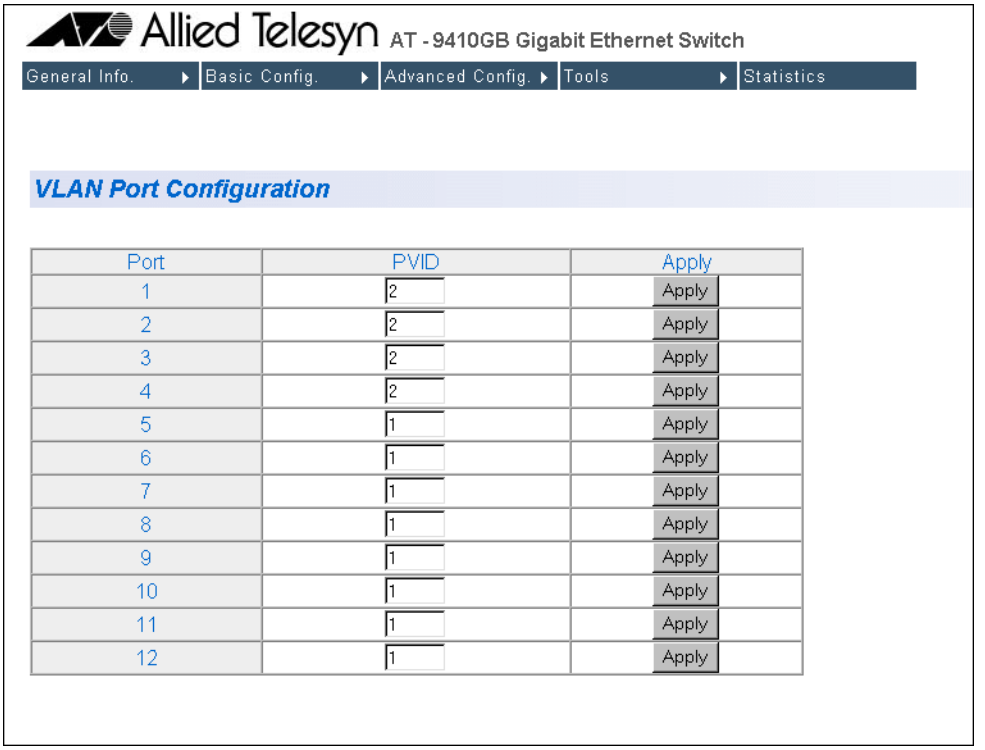

Figure 68 VLAN Port Configuration

This window lists the ports on the switch and each port's current PVID assignment. For example, referring to the figure above, Ports 5 to 12 all have a PVID of 1, meaning that they are untagged members of the Default VLAN, which has a VID of 1.

2. Enter a PVID value in the PVID field for the port number whose PVID you want to change.

   Once a new PVID has been assigned to a port, the port is removed as an untagged port from its current VLAN and added to the new VLAN as an untagged port.

   If the port is also an tagged member of any VLANs, it remains as a tagged member of those VLANs.

3. Click **Apply**.
4. Repeat steps 2 and 3 to assign new PVIDs to any other ports that are to be untagged members of the new VLAN.

This completes the procedure for creating a new VLAN.

Viewing or Modifying a Tagged or Untagged VLAN

There are two phases to modifying a VLAN. You might need to perform both phases or just one, depending on what it is you want to change in the VLAN. The phases are:

- ❑ Phase 1: In this phase, you can view a VLAN's configuration, as well as change a VLAN's name and add or remove tagged ports.
- ❑ Phase 2: In this phase, you can add or remove untagged ports.

Phase 1

This phase explains how to display the Config VLAN Member Menu of a VLAN. This window displays a VLAN's configuration. You can also use the window to change a VLAN's name and add or remove tagged ports.

Note
If you do not want to change a VLAN's name or add or remove tagged ports, then skip this procedure and go straight to Phase 2 to add or remove untagged ports.

1. On the Home page, select the **Advanced Config** menu tab and then select **VLAN Config** from the sub-menu. Select **VLAN Info** from the next sub-menu.

   The VLAN Information page will appear in Figure 69 as displayed.

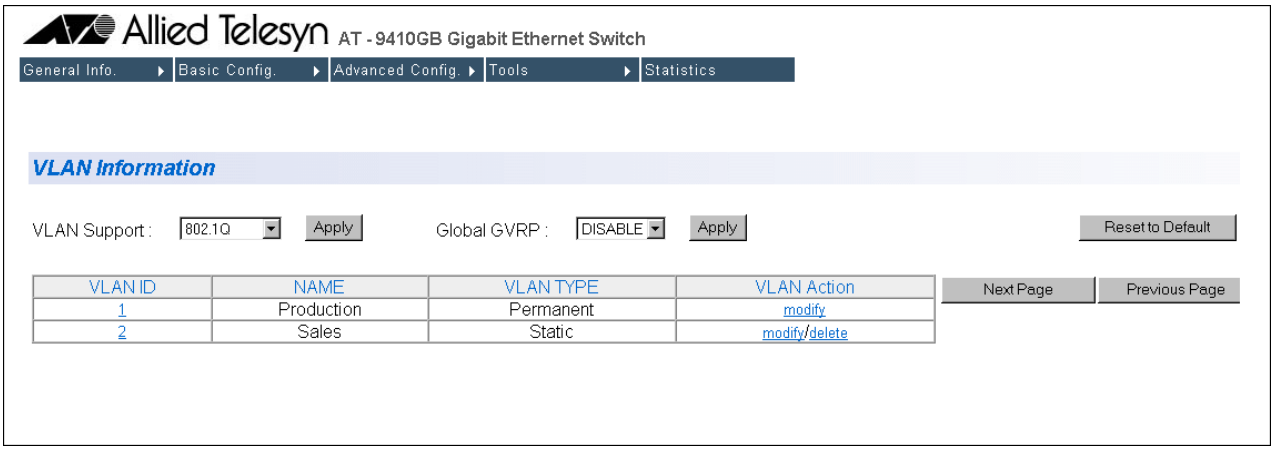

Figure 69 VLAN Information (802.1Q VLANs)

This window lists all of the tagged and untagged VLANs on the switch.

2. Click the **Modify** option located to the right of the VLAN you want to modify.

The VLAN Create/Modify (802.1Q VLANs) in Figure 70 is displayed.

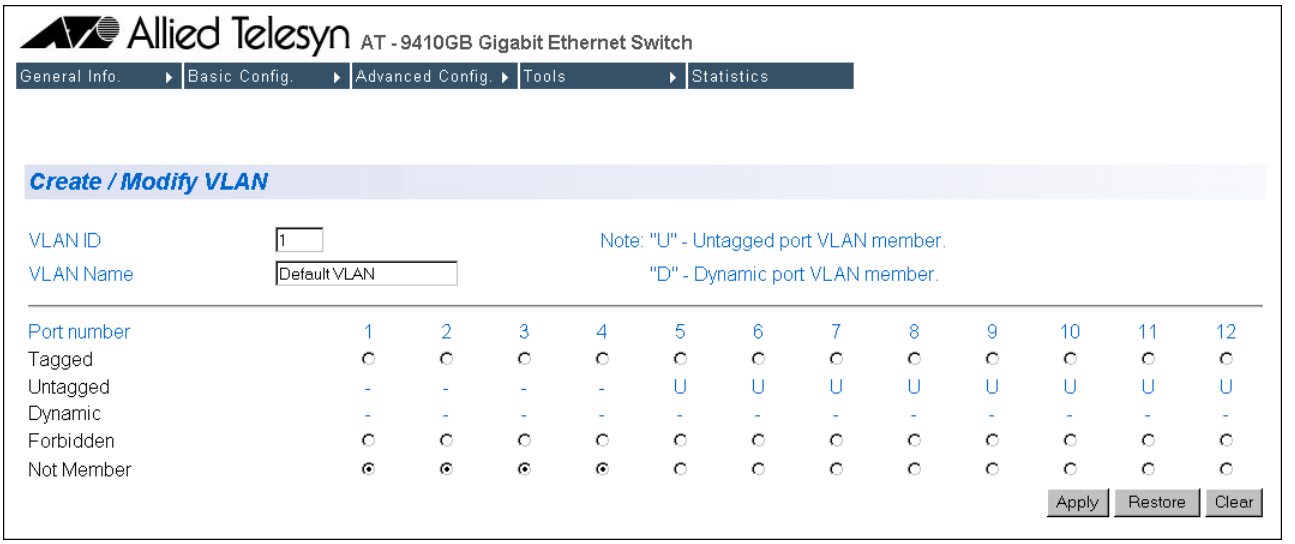
Allied Telesyn AT - 9410GB Gigabit Ethernet Switch
General Info.
Basic Config.
Advanced Config.
Tools
Statistics
Create / Modify VLAN
VLAN ID
1
VLAN Name
Default VLAN
Note: "U" - Untagged port VLAN member.
"D" - Dynamic port VLAN member.
Port number 1 2 3 4 5 6 7 8 9 10 11 12
Tagged
Untagged - - - - U U U U U U U U
Dynamic - - - - - - - - - - - -
Forbidden
Not Member
Apply
Restore
Clear

Figure 70 VLAN Create/Modify (802.1Q VLANs)

The rows on the page are defined below:

Tagged
A dot in a radio button indicates the corresponding port is a tagged member of the VLAN. For example, referring to the figure above, ports 9 and 10 on the master switch are tagged members of the VLAN.

Untagged
A 'U' for a port indicates that the port is an untagged member of the VLAN. For example, referring to the figure above, ports 1 through 8 on the master switch are untagged members of the VLAN.

Dynamic
tbd

Forbidden
A dot in a radio button indicates that the switch will not learn VLANs from the end node connected to the port. This applies only to tagged ports and only when GVRP has been activated on the switch.

Not Member
A selected radio button in this row indicates that the port is not a member of the VLAN.

3. To add a tagged port to the VLAN, click the Tagged radio button of the appropriate port.

Note
You cannot add untagged ports to a VLAN from this window. To add untagged ports, refer to **Phase 2**, below.

4. If you want to remove a tagged port from the VLAN, click the **Not Member** radio button of the appropriate port.

Note
You cannot remove untagged ports from a VLAN from this window. To remove untagged ports, refer to **Phase 2**, below.

5. If GVRP has been activated on the switch and you do not want the switch to learn new VLANs on a particular tagged port, click the Forbidden radio button of the appropriate tagged port.
6. After you have made the desired changes to the VLAN, click the **Apply** button.

Phase 2 You must perform this phase whenever you need to add or remove an untagged port from a VLAN. This phase explains how to change the PVIDs of the ports so that they match the VID of a different VLAN. For example, if you want to assign Port 2 as an untagged member of a VLAN with a VID of 4, you must change the PVID of the port to 4.

1. Click on the **Advanced Config** menu tab and select **VLAN Config** from the sub-menu. Select **VLAN Port Config** from the next sub-menu.

   The VLAN Port Configuration page will appear, as displayed in Figure 71.

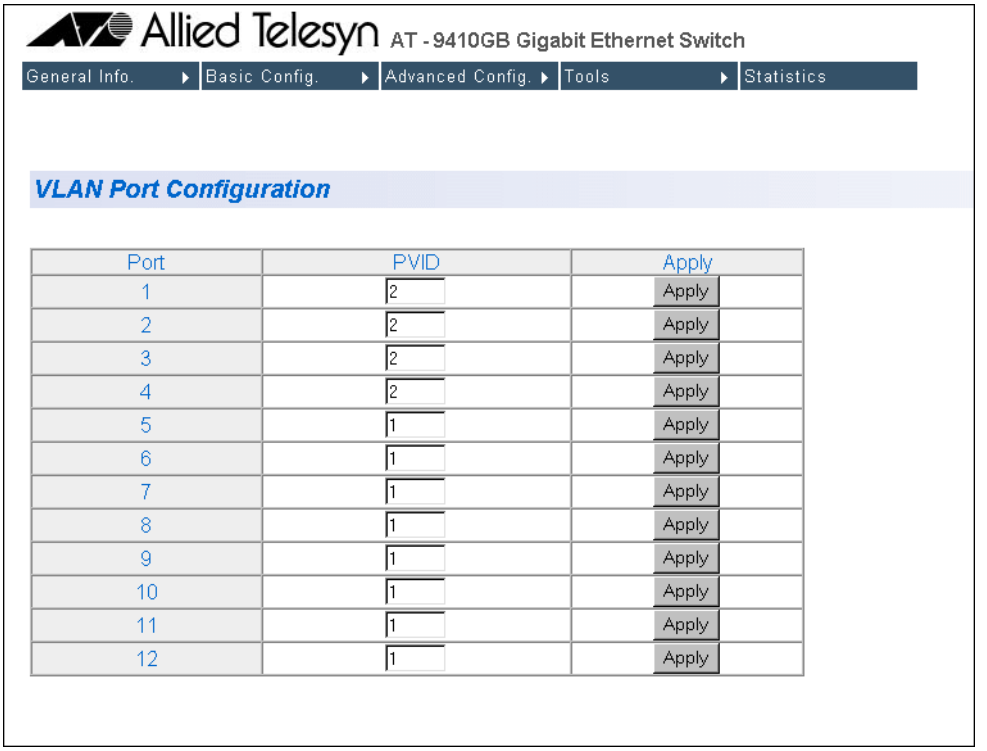

Figure 71 VLAN Port Configuration

This page lists the ports on the switch and each port's current PVID assignment. For example, referring to the figure above, Ports 5 to 12 all have a PVID of 1, meaning that they are untagged members of the Default VLAN, which has a VID of 1.

By default, this page initially displays the PVIDs for the ports on the master switch.

2. Enter a new **PVID** value in the PVID field for the port number whose PVID you want to change.

For example, if you wanted to make Port 4 an untagged port of a VLAN with a VID of 7, you would change the PVID for Port 4 to the value 7.

3. Click the **Apply** button.

   Once a new PVID has been assigned to a port, the port is removed as an untagged port from its current VLAN and added to the other VLAN as an untagged port.

   If the port is also an tagged member of any VLANs, it remains as a tagged member of those VLANs.

4. Repeat steps 2 and 3 to assign new PVIDs to any other ports on the switch that are to be untagged members of the VLAN.

This completes the procedure for modifying a VLAN.

Deleting a Tagged or Untagged VLAN

To delete a VLAN, perform the following procedure:

1. On the Home page, select the **Advanced Config** menu tab and then select **VLAN Config** from the sub-menu. Select **VLAN Info** from the next sub-menu.

   The VLAN Information page in Figure 72 is displayed.

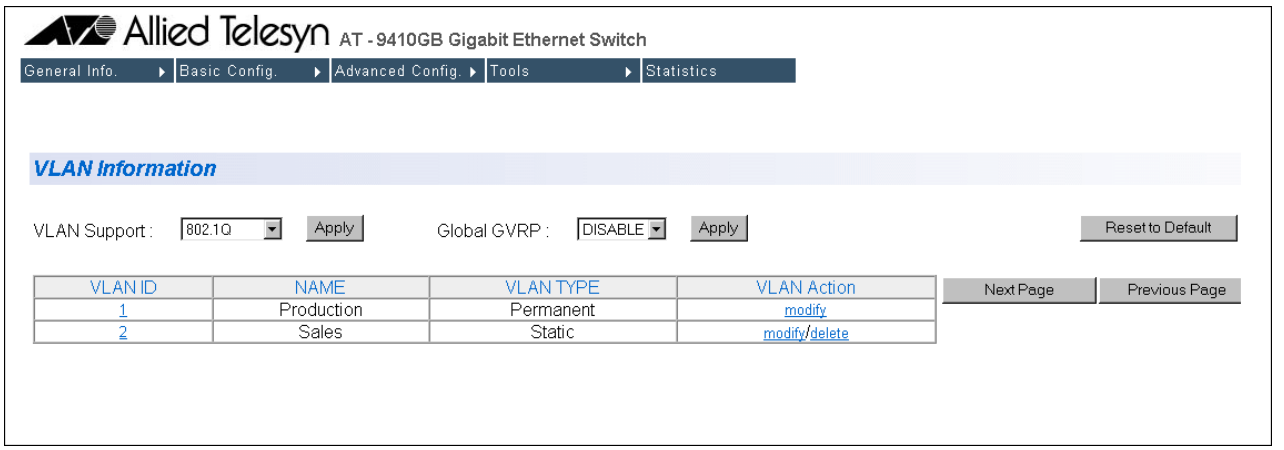

Figure 72 VLAN Information

2. Click the **Delete** option located to the right of the VLAN you want to delete.

   A confirmation prompt is displayed in Figure 73.

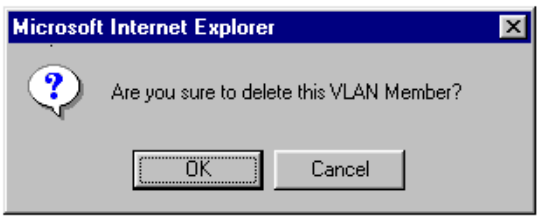

Figure 73 Confirmation Prompt

3. Click **OK**.

   The VLAN is removed from the switch. The PVIDs of the untagged ports in the VLAN are changed to 1, making the ports untagged members of the Default VLAN.

Note
You cannot delete the Default VLAN, which has a VLAN ID of 1.The Default VLAN is a permanent VLAN.

Creating a Port-based VLAN

To create a new port-based or VLAN, perform the following procedure:

> **Note**
> This procedure assumes that the switch is already running in the Port-based VLAN mode. For instructions on how to change the VLAN mode of the switch, refer to **Setting the VLAN Type** on page 218.

1. On the Home page, select the **Advanced Config** menu tab and then select **VLAN Config** from the sub-menu. Select **VLAN Create** from the next sub-menu.

   The Create/Modify VLAN page in Figure 72 is displayed.

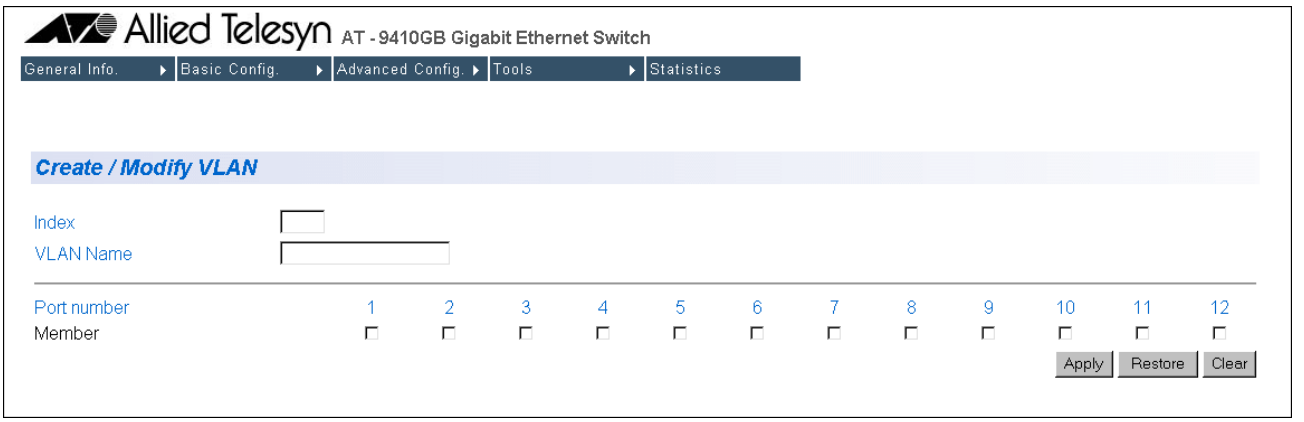

Figure 74 Create/Modify VLAN

2. Enter a unique VID in the Index field for the new VLAN. The VID can be between 2 and 4094.

   Since the switch does not examine the VID in tagged headers of tagged frames when operating in the Port-based VLAN mode, this VID value does not need to be unique from all other VLANs in your network. It only needs to be unique from the other VLANs in the switch on which you are creating the VLAN.

3. Enter a name for the new VLAN in the VLAN Name field. The VLAN name can contain 0 to 32 characters.

   The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!). Then press Enter.

4. Click the ports from the Port Number Member field which you want to add to the new VLAN.

   The VLAN must include at least one port.

Note
The ports that you add to the new VLAN are not removed from their current VLAN assignments. You must remove the ports manually from the other VLANs if you do not want them to be shared. For instructions, refer to **Viewing or Modifying a Port-based VLAN** on page 214.

5. Click **Apply**. This will save the VLAN you have just created and make it visible in the VLAN Info Menu.

Note
There are two additional buttons in the bottom right-hand corner of the page. The Restore button will cancel any changes you have made to the VLAN since using the Apply button. The Clear button removes all check marks from all check boxes, letting you re-start the port selection process.

You can repeat this procedure to create additional port-based VLANs.

Viewing or Modifying a Port-based VLAN

To view the configuration of a port-based VLAN or to modify a VLAN, such as to add or remove ports or to change the VLAN name, perform the following procedure:

1. Click on the **Advanced Config** menu tab and select **VLAN Config** from the sub-menu. Select **VLAN Info** from the next sub-menu.

   The VLAN Information page will appear, as displayed in Figure 75

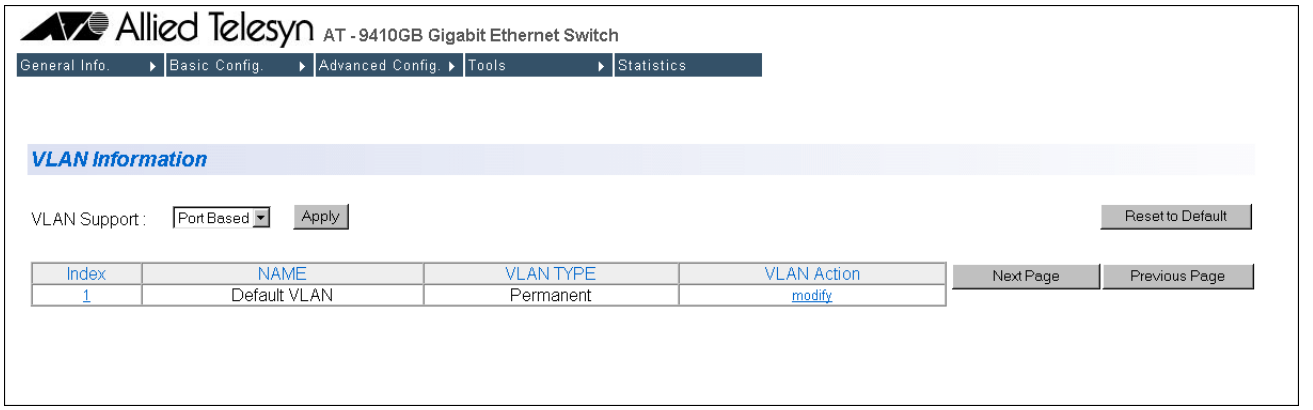

Figure 75 VLAN Information (Port-based)

   This page lists the port-based VLANs on the switch.

2. Click the Modify link in the right column for the VLAN you want to view or modify.

   The Create/Modify VLAN page will appear, as displayed in Figure 76.

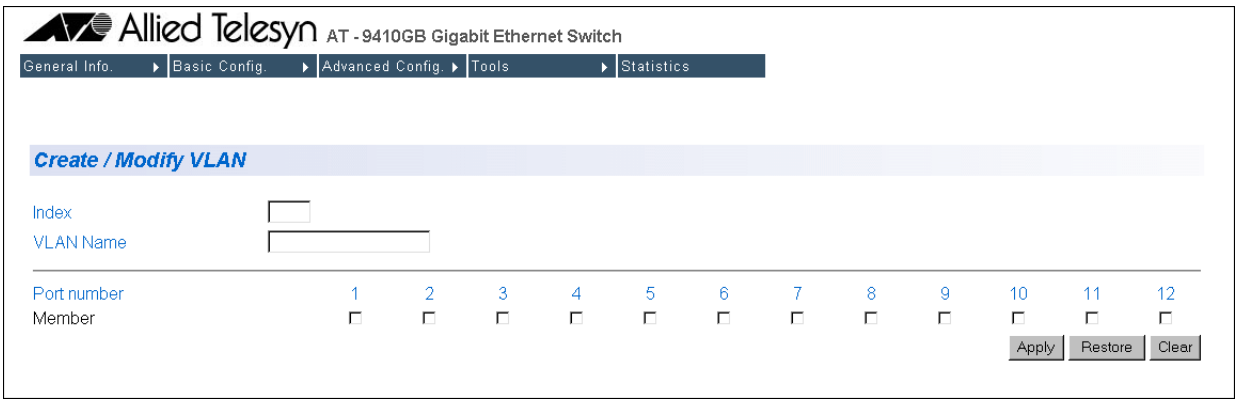

Figure 76 Create/Modify VLAN (Port-based VLANs)

The page indicates which ports on the switch which are members of the VLAN. A check in a check box indicates that the port is a VLAN member. An empty box indicates that the port is not a VLAN member.

3. To change the VLAN's name, enter a new name in the VLAN Name text entry field. The name can be from 1 to 32 characters. The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!). This menu item is optional; the management software does not require you to provide VLAN names.
4. To add or remove a port, click on the appropriate check box.

Note
You cannot remove ports from the Default VLAN unless they already belong to another VLAN. Additionally, port removed from other VLANs are returned to the Default VLAN.

Setting GVRP Status

Note
Global GVRP is not supported in port-based VLAN mode.

To set the GVRP status, perform the following procedure:

1. Click on the **Advanced Config** menu tab and select **VLAN Config** from the sub-menu. Select **VLAN Info** from the next sub-menu.

   The VLAN Information page in Figure 77 is displayed.

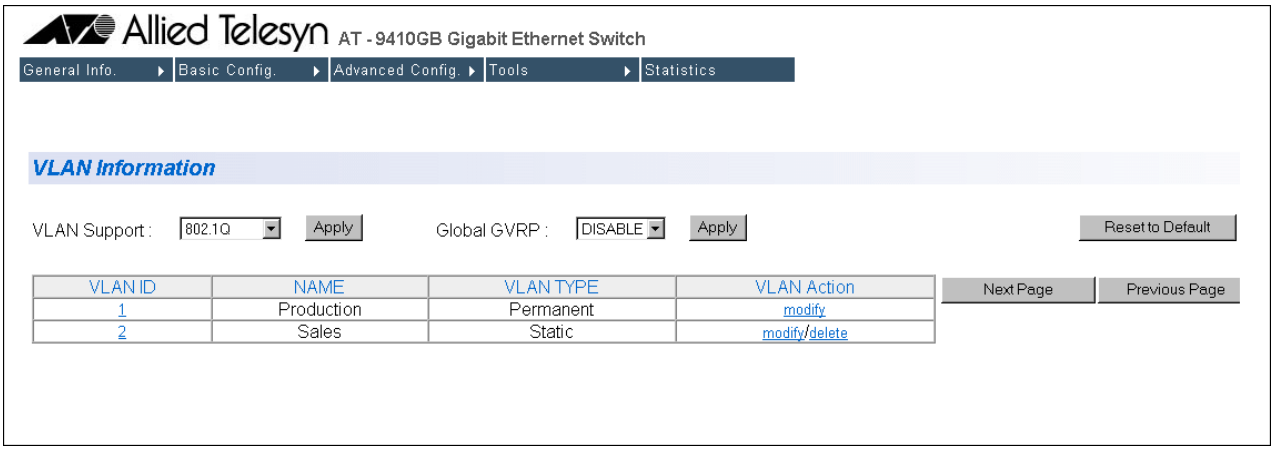

Figure 77 VLAN Information

2. Click on the Global GVRP pull-down menu, select **Enable**.

Note
The default is disable.

3. Click the **Apply** button.

Resetting the VLAN Parameters to Default

This command deletes all VLANs that you created. All ports are returned back to the Default VLAN.

To return the VLAN parameters of the switch to their default settings, perform the following procedure:

1. Click on the **Advanced Config** menu tab and select **VLAN Config** from the sub-menu. Select **VLAN Info** from the next sub-menu.

   The VLAN Information page in Figure 78 is displayed.

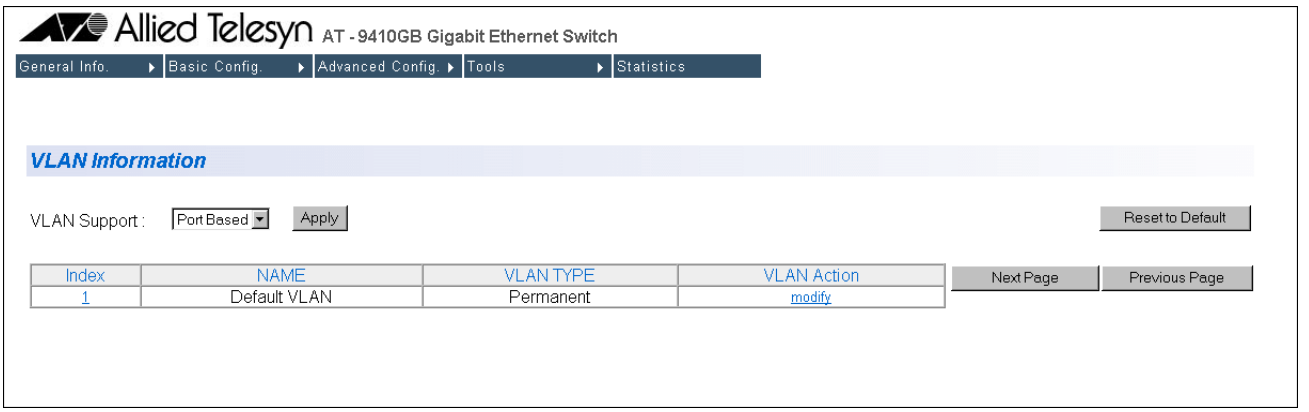

Figure 78 VLAN Information

2. Click on the **Reset to Default** button on the right side of the page.

   A confirmation prompt is displayed.

3. Click the **OK** button.

Setting the VLAN Type

The AT-9410GB switch can operate in either the 802.1Q VLAN mode for creating tagged and untagged VLANs or the port-based VLAN mode.

Note
The VLAN Type default is 802.1Q.

To change the switch's VLAN Type, perform the following procedure:

1. Click on the **Advanced Config** menu tab and select **VLAN Config** from the sub-menu. Select **VLAN Info** from the next sub-menu.

   The VLAN Information page will appear.

2. Using the VLAN Support pull-down menu, select either 802.1Q to create tagged and untagged ports or Port Based to create port-based VLANs.

   Note
   The default is 802.1Q.

3. Click the **Apply** button.

   Note
   Changing the VLAN Type setting deletes all VLANs except the Default VLAN.

Chapter 24

MAC Address Table

This chapter contains instructions on how to view the dynamic and static addresses in the MAC address table of the switch. This chapter contains the following procedure:

- ❑ **Viewing the MAC Address by Port** on page 221
- ❑ **Viewing the MAC Addresses by MAC** on page 222
- ❑ **Viewing the MAC Addresses of a VLAN** on page 224
- ❑ **Adding Static MAC Addresses** on page 226
- ❑ **Deleting Static MAC Addresses** on page 227

Note
For background information on the MAC address table, refer to **MAC Address Overview** on page 113.

Viewing the MAC Address by Port

This section contains the procedure for viewing the dynamic MAC addresses that have been learned on a particular port. You can also use this procedure to view any static MAC addresses that have been assigned to a port.

1. On the Home page, select the **Basic Config** menu tab and then select the **Forwarding DB** tab from the sub-menu. Select **Sort by Port** from the next sub-menu.

   The Sort by Port window will appear, as displayed.

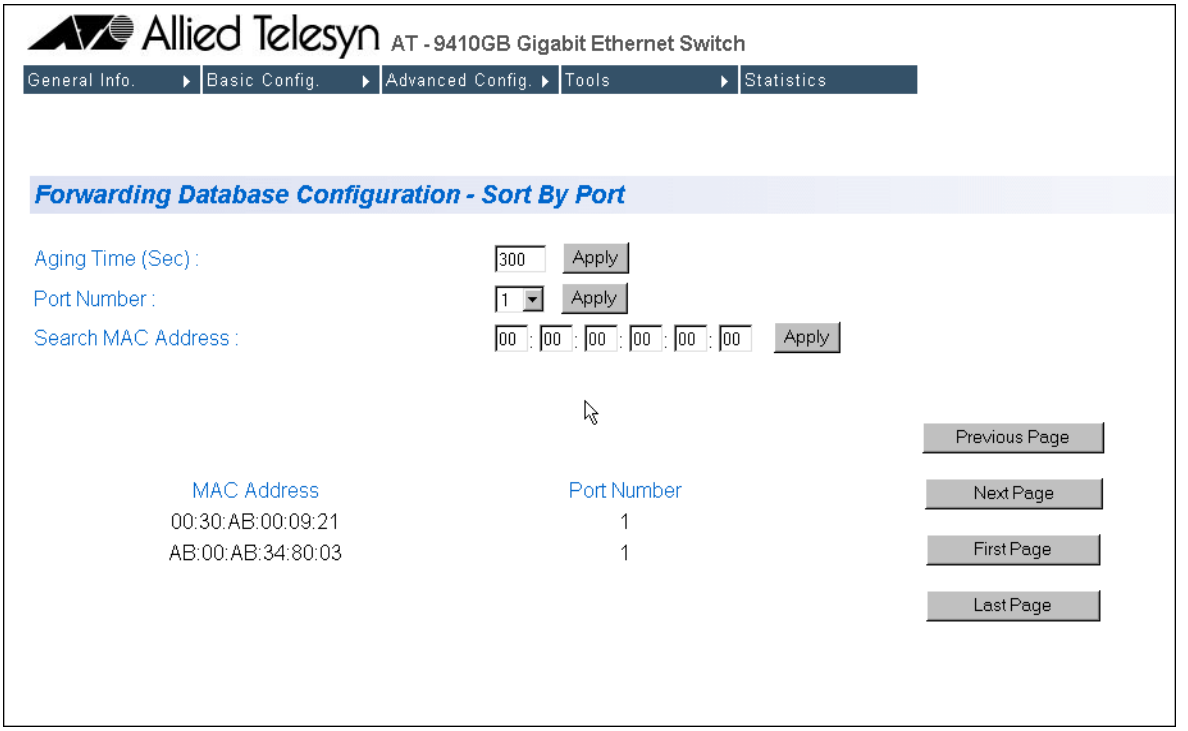

Figure 79 Sort by Port Window

2. Select the port whose static and dynamic MAC addresses you want to view from the Port Number pull-down menu.
3. Select **Apply** from the menu next to the Port Number.

   A window is displayed with the MAC addresses of the nodes on the port. The columns in the window and the definitions of the columns are the same as for the Display MAC Address by MAC window on page 113.

Viewing the MAC Addresses by MAC

This section contains the procedure for viewing the dynamic MAC addresses that have been learned on all ports of a switch. This procedure will also let you view all static MAC addresses that have been assigned to the ports on the switch.

To view the MAC addresses in numerical order on the switch, perform the following procedure.

1. On the Home page, select the **Basic Config** menu tab and then the **Forwarding DB** tab from the sub-menu. Select **Sort by MAC** from the next sub-menu.

   The Forwarding Database Configuration - Sort by MAC window will appear, as displayed.

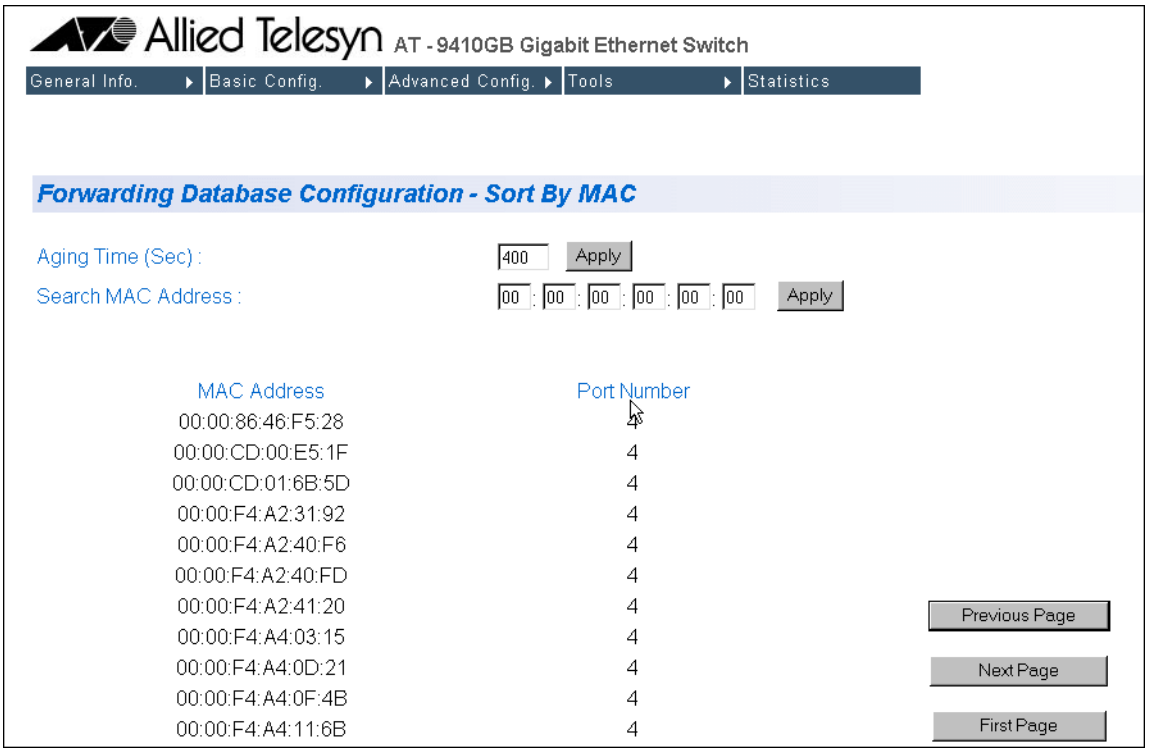

Figure 80 Sort by MAC Window

   The management software displays a window with a list of all static and dynamic MAC addresses of the nodes of all ports. For definitions of the columns, refer to the Display MAC Address by MAC window on page 113.

2. To search by MAC address, enter a MAC address into the Search MAC Address field. Click **Apply**.

The window displays the corresponding port number where the end node is connected.

3. To modify the aging time, enter a value in seconds in the Aging Time field. The Aging setting is in range of 10 to 1048 seconds. The default setting is 300 seconds.
4. Click **Apply**.

   The management software immediately activates the new aging time value on all ports of the switch.

   For more instructions on the setting Aging, please refer to **Changing the Aging Time** on page 122

Viewing the MAC Addresses of a VLAN

The procedure in this section can be useful if you created VLANs on the switch and want to view the MAC addresses of the nodes of a particular VLAN. (This procedure is not of much value if the switch contains only the Default VLAN, in which case displaying the entire MAC address table, as explained earlier in this chapter, produces the same result.)

Note
To perform this procedure, you need to know the VID number of the VLAN whose MAC addresses you want to view.

Note
Viewing MAC Addresses by VLAN is not supported in port-based VLAN mode.

To view the MAC addresses of a VLAN on the switch, perform the following procedure.

1. On the Home page, select the **Basic Config** menu tab and then select the **Forwarding DB** tab from the sub-menu. Select **Sort by VLAN** from the next sub-menu.

   The Forwarding Database Configuration - Sort by VLAN window will appear, as displayed.

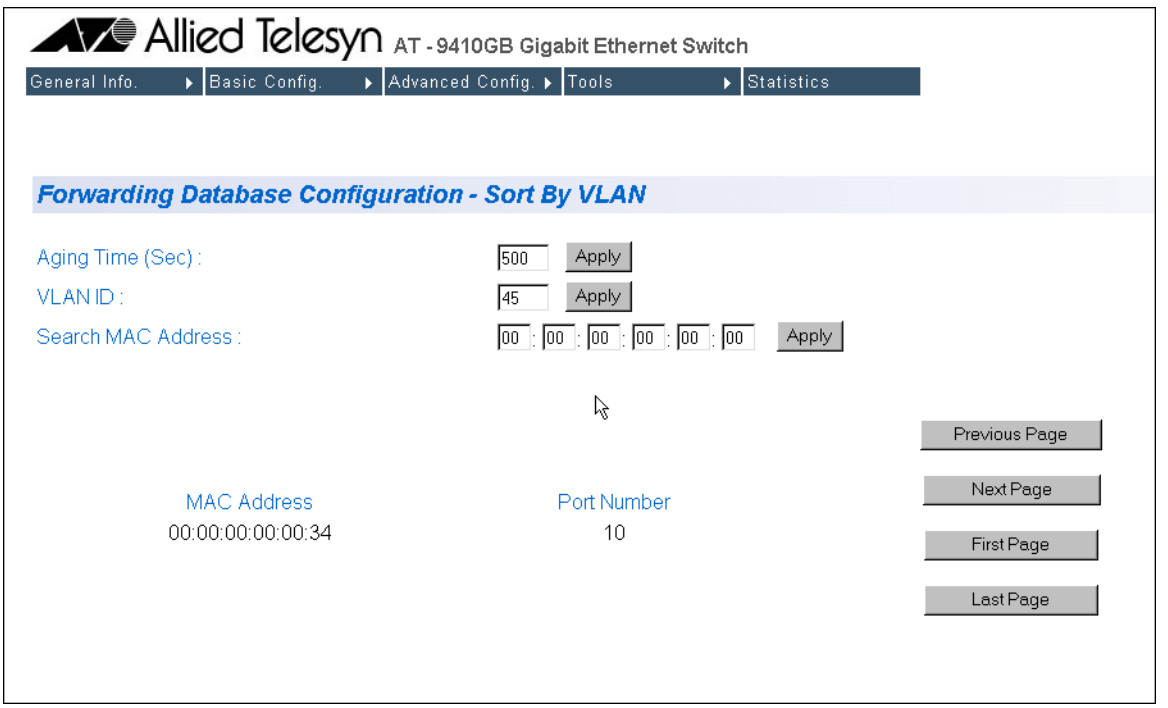

Figure 81 Forwarding Database Configuration - Sort by VLAN Window

2. Enter the VLAN ID whose static and dynamic MAC addresses you want to view into the VLAN ID field.
3. Click the **Apply** button next to the VLAN ID field.

   The management software displays the MAC addresses of the nodes of all ports in the VLAN.
4. To modify the aging time, enter a value in seconds in the Aging Time field. The Aging setting is in range of 10 to 1048 seconds. The default setting is 300 seconds.
5. Click **Apply**.

   The management software immediately activates the new aging time value on all ports of the switch.

Adding Static MAC Addresses

The management software allows you to assign up to 254 static MAC addresses per port on an AT-9410GB Gigabit Ethernet Switch.

To add a static address to the MAC address table, perform the following procedure:

1. On the Home page, select the **Basic Config** menu tab and then select the **Forwarding DB** tab from the sub-menu. Select **Static FDB** from the next sub-menu.

   The Static MAC Address Configuration window will appear, as displayed.

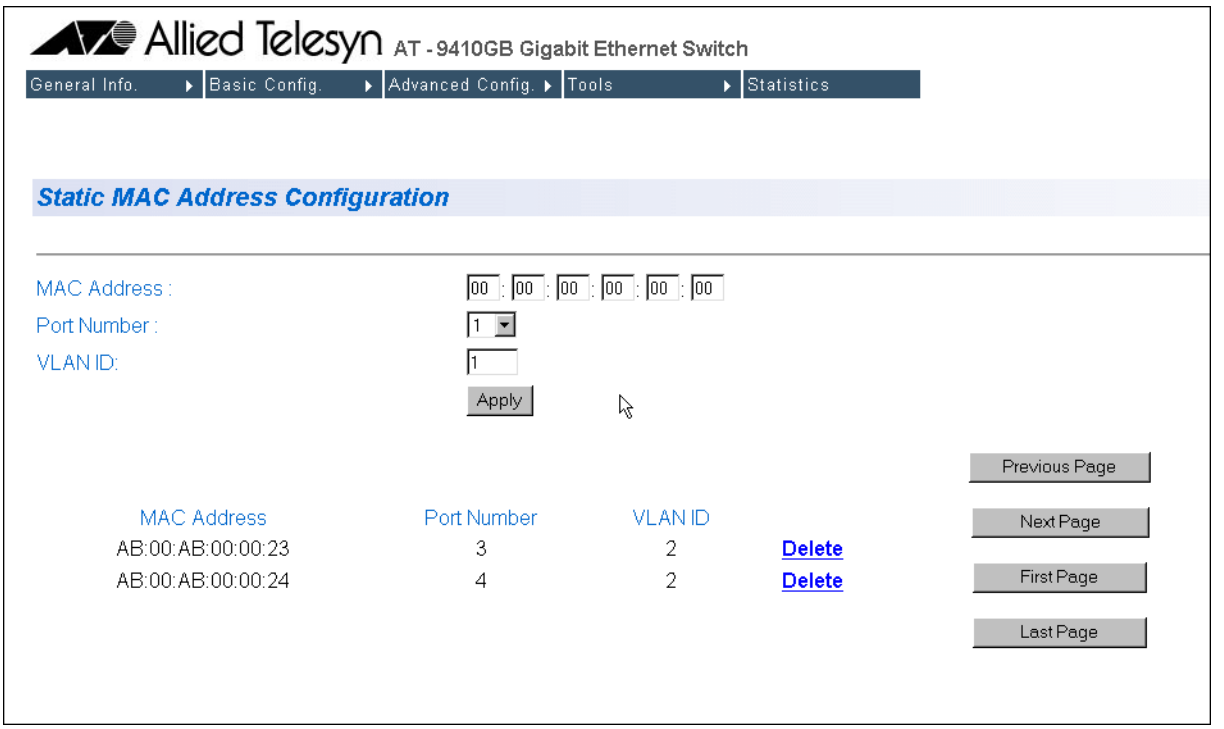

Figure 82 Static MAC Address Configuration Window

2. Enter a MAC Address you want to configure in the MAC Address field.
3. Click on the Port Number pull-down menu and select the port number you want to configure.
4. Enter a VLAN ID value in the VLAN ID field.
5. Click **Apply**.

   The management software adds the static address to the MAC address table for the specified port and VLAN.
6. Repeat steps 2 and 5 to enter additional static MAC addresses.

Deleting Static MAC Addresses

To delete a static MAC address, perform the following procedure:

1. On the Home page, select the **Basic Config** menu tab and then the **Forwarding DB** tab from the sub-menu. Select **Static FDB** from the next sub-menu.

   The Static MAC Address Configuration window will appear, as displayed.

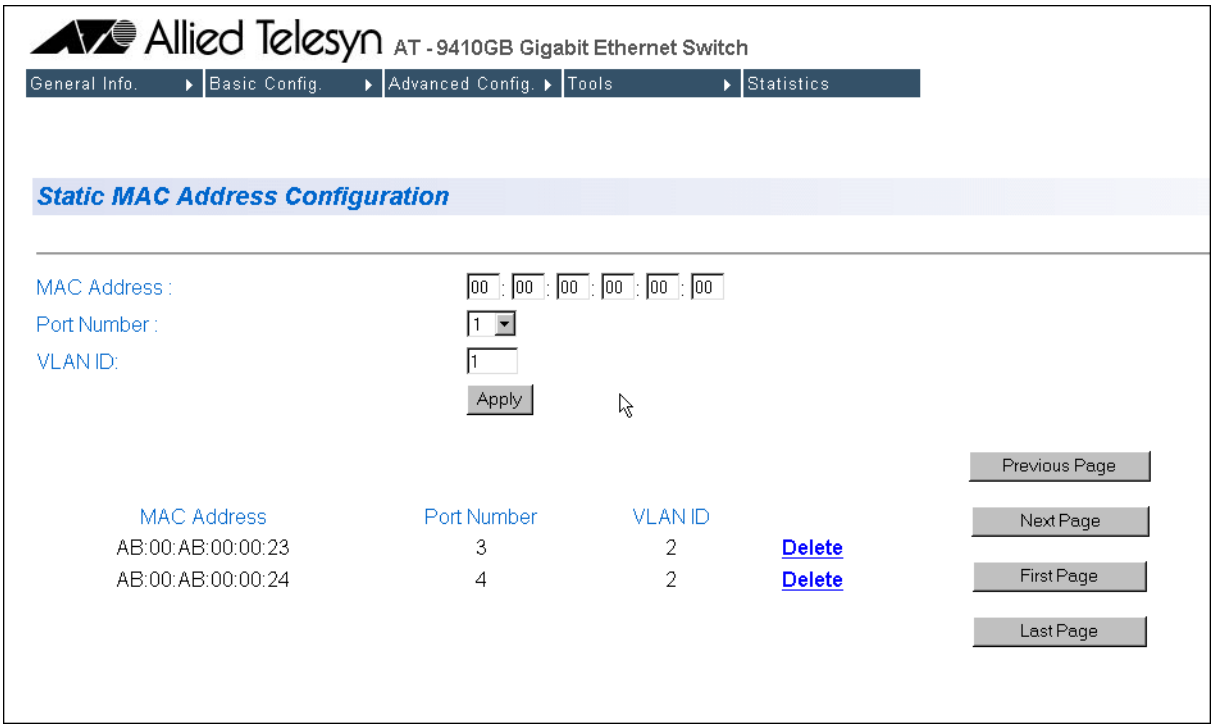

Figure 83 Static MAC Address Configuration Window

   The management software displays all static addresses from the MAC address table.

2. Select the **Delete** field on the right side of the window for the MAC Address you desire to delete.

   The management software deletes the static address you have selected from the MAC address table.

3. Repeat step 2 to delete additional static MAC addresses.

Chapter 25
Quality of Service

This chapter contains instructions on how to configure QoS. This chapter contains the following procedure:

- ❑ **Configuring QoS** on page 229

Note
For background information on QoS, refer to **Quality of Service Overview** on page 124.

Configuring QoS

Note
Quality of Service is not supported in port-based VLAN mode.

To configure QoS, perform the following procedure:

1. From the Home page, select **Advanced Config.** and then select **Quality of Service** from the sub-menu.

   The management software displays the Quality of Service window in Figure 84.

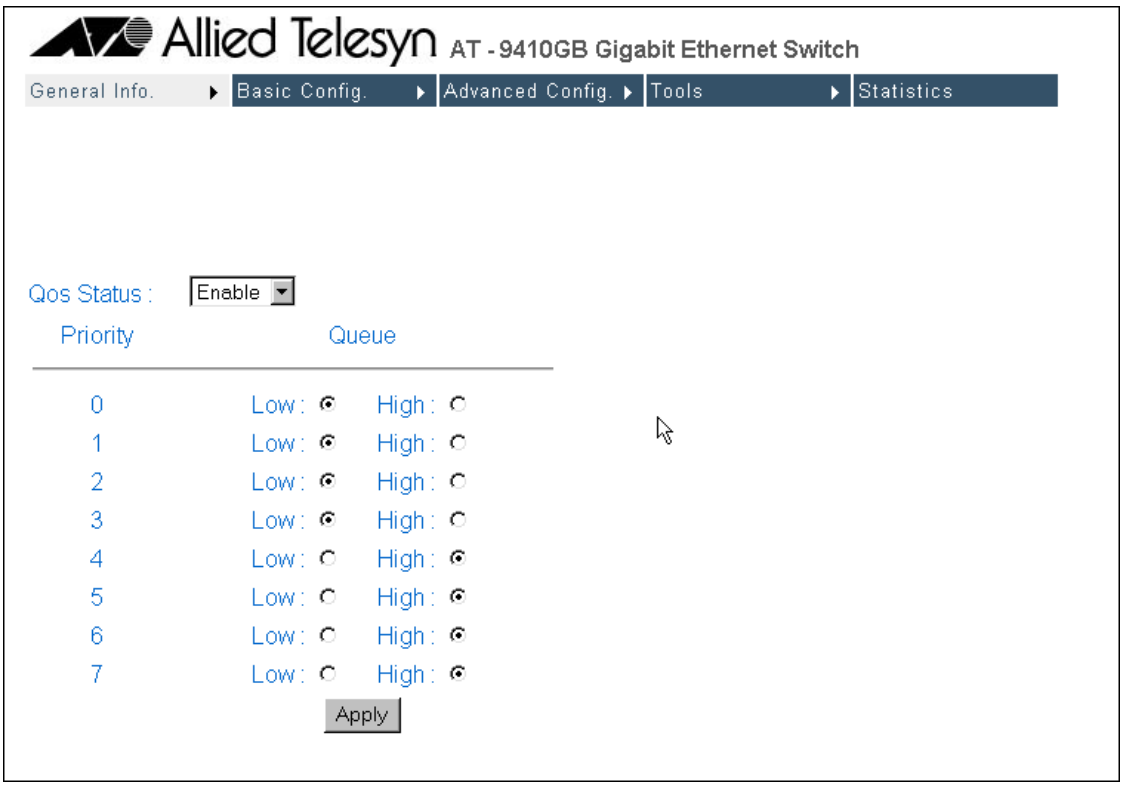

Figure 84 Quality of Service Window

1. Select a Low or High priority queue for the traffic classes whose priority you wish to change.

   Note
   The default setting for traffic classes 0 - 3 is the low priority queue. The default setting for traffic classes 4 - 7 is the high priority queue.

2. Select **Enable** from the QoS Status pull-down menu.
3. Click the **Apply** button.

All tagged frames will be directed to either the low or high priority queue specified in Step 2.

Note
The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame exits the switch with the same priority level that it had when it entered.

Chapter 26
IGMP Snooping

This chapter explains how to activate and configure the IGMP snooping feature on the switch. Sections in the chapter include:

- ❑ **Activating IGMP Snooping** on page 233
- ❑ **Viewing Group Members** on page 235

Note
For background information on this feature, refer to **IGMP Snooping** on page 128.

Activating IGMP Snooping

To enable or disable IGMP snooping on the switch and to configure IGMP snooping parameters, perform the following procedure:

1. Click on the **Advanced Config** menu tab and select **IGMP Snooping** from the sub-menu.

   The IGMP Snooping page will appear, as displayed in Figure 85.

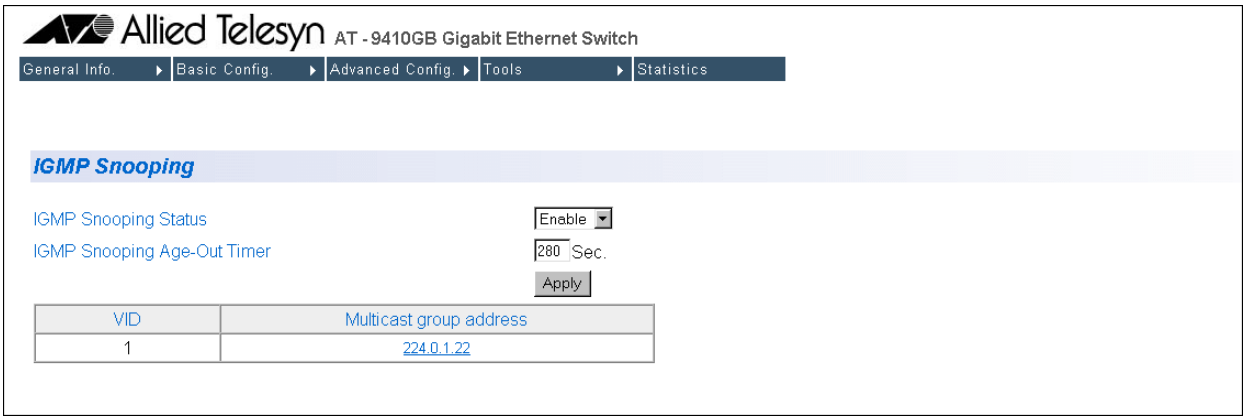

Figure 85 IGMP Snooping

The parameters on the IGMP Snooping page are defined below:

IGMP Snooping Status
Enables and disables IGMP snooping on the switch.

After selecting Enable or Disable, click the Apply button below the pull-down menus.

Age Out Timer
Specifies the time period in seconds after which the switch stops sending out multicast packets out of a port with an inactive host node. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 280 to 420 seconds. The default is 280 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.

After entering a new time, click the Apply button below the pull-down menus.

VID
The VLAN ID of the VLAN the multicast group belongs to. This parameter will only be visible if you have created a VLAN.

Multicast Group Address
The multicast address of the group.

To view the members of the multicast group, click on the multicast address.

Viewing Group Members

You can use the AT-S45 software to display a list of the members of each multicast group on a switch. To display the list, perform the following procedure:

1. Click on the **Advanced Config** menu tab and select **IGMP Snooping** from the sub-menu.

   The IGMP Snooping page will appear, as displayed in Figure 85 on page 233.

2. Click on a multicast group address. The group members wil appear on the IGMP Snooping Group Members page, as displayed in Figure 86.

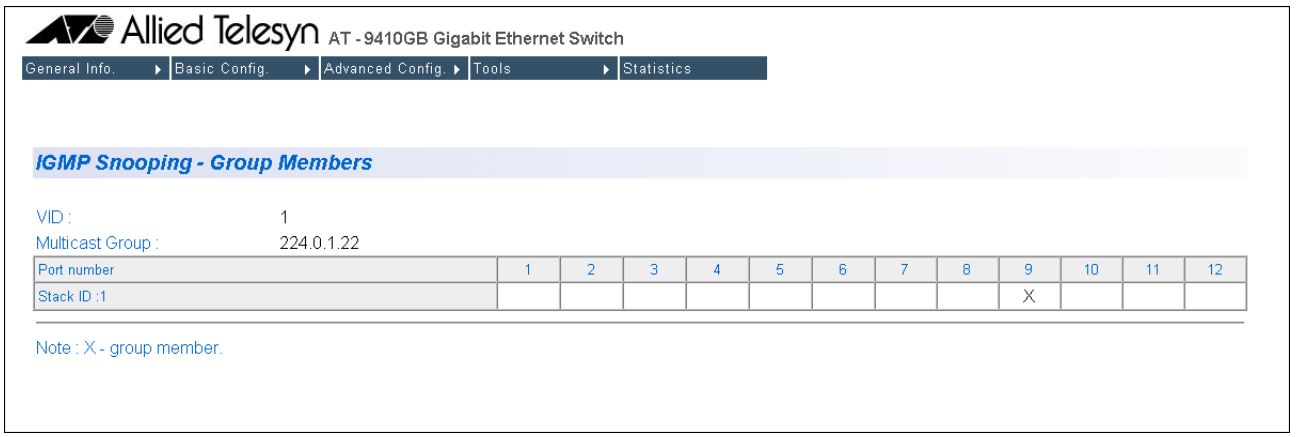
Allied Telesyn AT - 9410GB Gigabit Ethernet Switch
General Info.
Basic Config.
Advanced Config.
Tools
Statistics
IGMP Snooping - Group Members
VID : 1
Multicast Group : 224.0.1.22
Port number 1 2 3 4 5 6 7 8 9 10 11 12
Stack ID :1 X
Note : X - group member.

Figure 86 IGMP Snooping Group Members

The information on this page is for viewing purposes only. The parameters are defined below:

VID
The VLAN ID of the VLAN the multicast group belongs to. This parameter will only be visible if you have created a VLAN.

Multicast Group Address
The multicast address of the group.

Port Number
The ports on the switch.

Stack ID
The stack ID of the switch. An X in this row indicates that the port in the corresponding column is a member of this multicast group.

Chapter 27
Storm Control Configuration

This chapter contains instructions on how to configure the broadcast frame control feature on the switch.

Note
For background information on this feature, refer to **Storm Control Overview** on page 136.

Activating Broadcast Storm Control and Setting a Threshold

To activate storm control and set a threshold, perform the following procedure:

1. On the Home page, select the **Advanced Config** menu tab and then select **Storm Control** from the sub-menu.

   The Broadcast Storm Control page will appear, as displayed in Figure 87.

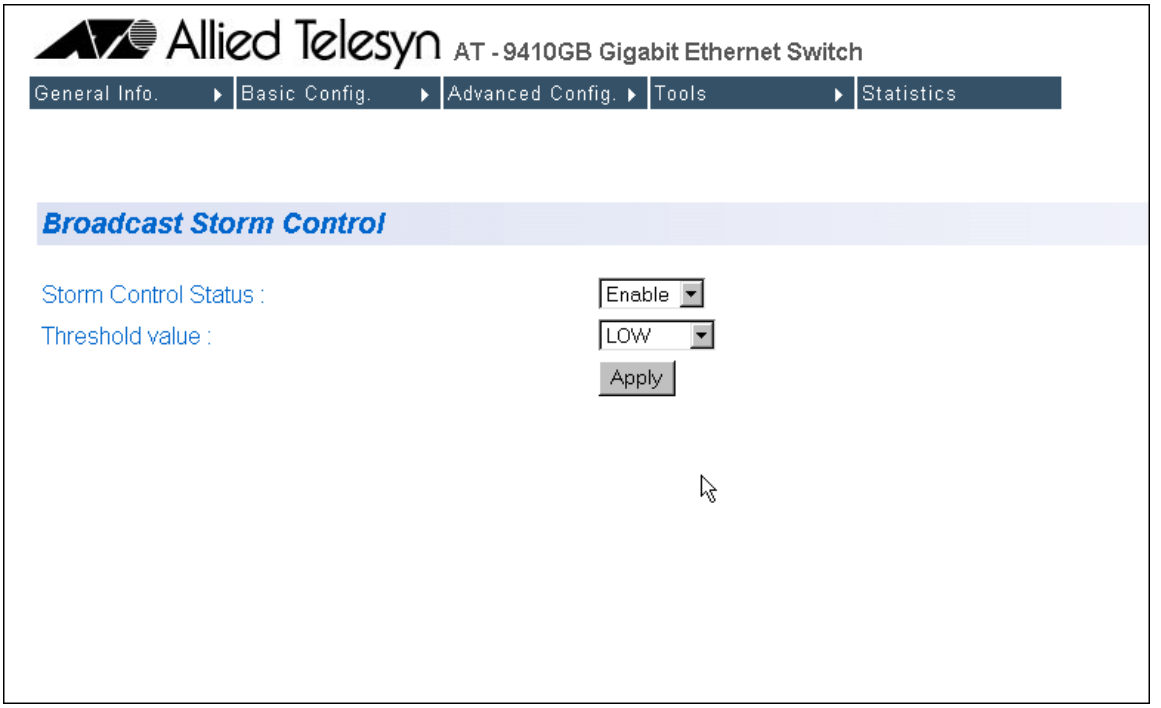

Figure 87 Broadcast Storm Control Window

2. From the Storm Control Status pull-down menu, select the **Enable** option.
3. To set the threshold, select an option from the Threshold value pull-down menu: **Low**, **Medium**, or **High**. If you do not select a threshold value, the switch will retain the default setting of **Low**.

   Note
   For an explanation of broadcast storm control threshold values, please **Storm Control Overview** on page 136.

4. Click the Apply button located below the pull-down menus to save your configuration options.

Chapter 28
Management Software Updates

This chapter explains how to obtain new versions of the AT-S45 management software and how to download the software onto an AT-9410GB switch.

You can download new management software onto a switch using the following method:

- Trivial File Transfer Protocol

Sections in the chapter include:

- **Obtaining Software Updates** on page 240
- **Downloading a New Management Software Image Using TFTP** on page 241

Obtaining Software Updates

New releases of the AT-S45 management software are available from the Allied Telesyn web site at www.alliedtelesyn.com and from our FTP server at ftp.alliedtelesyn.com. To log on to the FTP server, enter "anonymous" for the user name and your email address for the password. Management software for the AT-9410GB switch will have "S45" as part of the filename.

Downloading a New Management Software Image Using TFTP

TFTP software is available from various sources and is included in SNMP which can be purchased through Allied Telesyn. A command line version is included in most UNIX variants and in Windows NT. Please consult the documentation or the manufacturer of the software used on the proper use of the software.

You will need to provide the following information when using the TFTP client software to download the AT-S45 software image:

- ❑ Download Server IP
- ❑ Download File Name

This procedure assumes that you have already obtained a copy of TFTP software and have stored it on the computer from which you will be performing this procedure.

To download the new AS-45 software image onto your AT-9410GB switch, perform the following procedure:

1. Establish a web management session on the switch where you intend to download the new management software.

   For instructions, refer to **Starting a Web Browser Management Session** on page 154.

1. On the Home page, click on the **Tools** menu tab. The Tools sub-menu will appear. Choose **Image Upgrade** from the sub-menu.

   The Image Upgrade page will appear, as displayed.

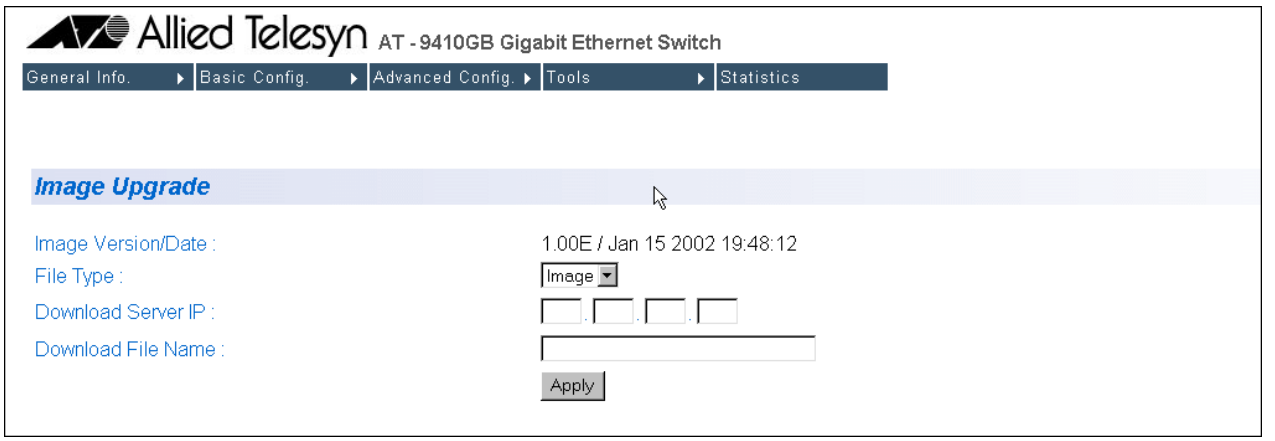

Figure 88 Image Upgrade Page

The options in the window are defined below.

Image Version/Date
The software version and date currently on the switch.

File Type

- **Image**
  An image file is the management software for the switch.

- **Configuration**
  A configuration file is a file that contains all of the existing configurations and settings for a switch. You can upload the configuration file and modify the switch settings and then download the configuration file back to the switch or onto multiple switches that you want to have the same configurations. The switch(es) will then update their configuration(s) based on the settings in the configuration file.

- **Image and Configuration**
  This option allows you to download both the management software and the configuration file.

Download Server IP
This is the IP address of the server from which you are downloading the new software.

Download File Name
The filename of the software that is to be downloaded onto the switch. The filename of the software should be "ATS45.img". If necessary, change the filename of the image.

2. Type the IP address into the **Download Server IP** field.
3. Type the software image name into the **Download File Name** field.
4. Open the TFTP client to download the software image onto the switch.

   Once the TFTP software is opened, it immediately begins to listen for incoming requests and the syslog server is running.

   Step 5 illustrates how to perform the transfer using the Tftpd32 by Ph. Jounin program.

5. Using the TFTP client, select the current directory where the software image is located.

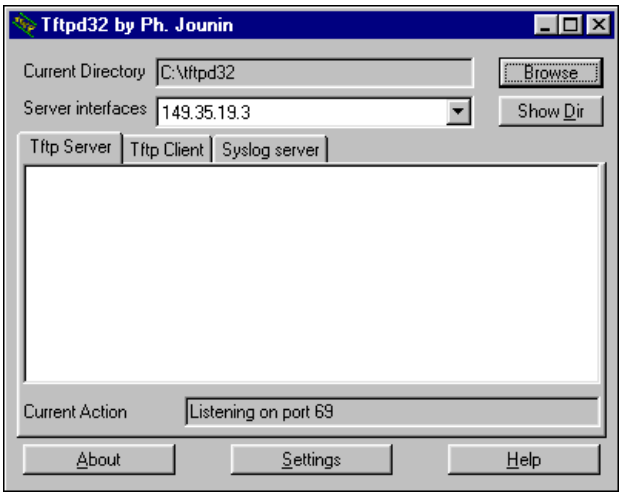

Figure 89 TFTP client software window

6. Return to the web management Software Upgrade page as displayed in Figure 88.
7. Click **Apply** to upgrade image.

   The software immediately begins to download onto the switch's CPU. This process will take seconds to complete.

   Once the new software download process has completed, the switch begins to initialize the software. This takes approximately 1 minute to complete. Once the initialization process is complete, the switch will automatically reboot.

Appendix A
AT-S45 Default Settings

This appendix lists the AT-S45 factory default settings.

Setting	Default
IP Address	0.0.0.0
Subnet Mask	255.255.0.0
Gateway Address	0.0.0.0
DHCP	Disabled
IGMP Snooping	Disabled
System Name	None
MAC Aging Time	300 seconds
Spanning Tree Protocol	
Status	Disabled
Bridge Priority	32768
Bridge Max Age Time	20
Bridge Hello Time	2
Bridge Forwarding Delay	15
Twisted Pair Ports	
Status	Enabled
Speed/Duplex Mode	Auto-Negotiate
Flow Control	Auto
Broadcast Storm Control	Disabled
MDI/MDI-X	Auto
Security	Normal
Port Monitoring	Disabled
Port Trunking	Disabled

Setting	Default
VLANs	
Port-based and Tagged VLANs	Enabled
VLAN Name	Default VLAN (all ports)
Default VLAN ID	1
RS-232 Terminal Port	
Emualtion Mode	VT100
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Data Rate	9600 bps
Key Mode	Terminal (not Windows)
Login Name	manager
Login Password	manager

Index

A
admin status, 178
aging time
    changing, 122
    defined, 114
AT-S45 default settings, 40, 245
AT-S45 software updates
    downloading from a local session, 145
    obtaining, 144, 240
AT-S45 version number, 46
Auto-Negotiation, 53, 178, 181

B
BOOTP
    defined, 36, 164
bootstrap
    configuration, 49
BPDU, *see* bridge protocol data unit
bridge identifier, 77
bridge priority, 77, 197
bridge protocol data unit (BPDU), 81, 197
broadcast frame control
    configuring, 135, 236
    defined, 136
browser tools, 155

C
Class of Service
    configuring, 125, 229
    defined, 124
console timeout, 43
console UI Idle Timeout
    changing, 162
conventions, used in this guide, 11

D
default values, AT-S45, 40, 245
DHCP
    activating, 36, 164
    defined, 36
        activating, 164
documentation, 12

F
flow control, 55, 178, 180
forwarding delay, 79, 82, 115, 197

G
gateway address, 33, 159

H
hello time, 79, 197
host nodes
    defined, 129
    displaying, 132, 235
host/router timeout interval, 130, 233

I
IEEE 802.1d standard, 80, 196
IGMP snooping
    configuring, 130, 233
    defined, 129
Internet Protocol (IP) address
    defined, 33

Internet Protocol (IP) address, 31, 158
interval timer
    configuring, 137

L
Limited level, port security, 58
limited security mode
    configuring, 61
    defined, 58
link status, 178
local management session
    defined, 20
    quitting, 28
    starting, 26

M
MAC address table, 112, 221
MAC address, switch, 46
Management Information Base (MIB), 23
managemet access methods, 43
multicast groups, maximum, 131

N
Normal level, port security, 58

P
password
    changing, 45
    default, 27, 29, 154
ping, 47
port
    configuring parameters, 54, 177
    disable, 54
    displaying status, 52, 179, 182
    speed, 55, 178, 181
port cost
    defined, 78
    setting, 83, 198
port index, 177
port mirroring
    creating, 193
    deleting, 193
port monitoring
    creating, 73
    defined, 72
    deleting, 75
port security
    configuring, 59
    defined, 58
    displaying, 186, 188
port statistics, 140
port trunking
    creating, 66, 190
    defined, 64
    deleting, 69, 190
port-based VLAN
    creating, 93, 98, 103, 105, 110, 111, 202, 206, 211, 212, 216, 217
    defined, 89
priority queues, 124
priority, 83, 198

Q
quitting
    local session, 28
    Telnet session, 29
    web browser session, 156

R
resetting a switch, 42, 168
root bridge, 77
RS232 port, default settings, 27

S
Secure level, port security, 58
serial number, switch, 46
SNMP Agent
    changing, 163
SNMP community strings, 38, 166
SNMP management session, 23
software updates
    downloading from a local session, 145
    obtaining, 144, 240
Spanning Tree Protocol
    configuring bridge parameters, 80, 196
    configuring port parameters, 83
    defined, 77
    port cost, 78, 83, 198
    viewing bridge parameters, 198
starting session
    local, 26
    Telnet, 29
    web browser, 154
static MAC address

adding, 120, 226
deleting, 121, 227
displaying, 115
statistics
port, 140
STP. See Spanning Tree Protocol
subnet mask, 33, 159
system name
defined, 34
system name, 160

T
tagged VLAN
creating, 105, 212
defined, 91
Telnet management session
defined, 21
quitting, 29
starting, 29
Telnet server
changing, 163
Telnet UI Idle Timeout
changing, 163
trunk, 177
type, 178

U
user name
changing, 45
user name and password
configuring 43
user name, default, 154

V
version number, AT-S45, 46
virtual LAN
creating, 93, 98, 103, 105, 110, 111, 202, 206, 211, 212, 216, 217
defined, 87
port-based, defined, 89
tagged, defined, 91
VLAN identifier (VID), 89
VLAN. See virtual LAN

W
web browser management session
limitations, 22
quitting, 156
starting, 154
Web server
changing, 163